5 AÇÕES DE CONTENÇÃO DE INTRUSOS COM SDN

Neste capítulo serão estudados os aspectos de contenção de intrusos através de mecanismos SDN. Nas próximas seções o leitor poderá entender as diferenças entre IDS e IPS, tipos de contenção que podem ser empregadas e como SDN poderá apoiar nessas ações.

5.1 Sistemas de Prevenção de Intrusos

No capítulo anterior foi possível ter uma visão geral sobre o funcionamento dos Sistemas de Detecção de Intrusão, cujo objetivo resume-se a monitorar a rede ou o host e identificar comportamentos maliciosos - tipicamente ataques. É possível fazer uma analogia do IDS com um sistema de alarme de um carro, que apenas soa uma sirene quando alguém abre o carro sem autorização. Neste capítulo, será abordado as ferramentas de IPS (Sistema de Prevenção de Intrusão) que tem uma ação mais incisiva ao receber os alertas do IDS. O IPS complementa, portanto, o funcionamento do IDS, uma vez que ele bloqueia a intrusão e impede que um dano maior seja causado à rede. Utilizando a analogia do carro, é como se o IPS, além de disparar o alarme, também trave as rodas para evitar que o invasor leve o carro. É possível pensar sobre o IDS como um sistema passivo (apenas detecta) e no IPS como um sistema ativo (detecta e atua sobre o evento).

Um exemplo de funcionamento do IPS é ilustrado na Figura 5.1. Nessa figura é importante notar que a rede da organização conta com um sistema de Firewall para filtragem dos pacotes e também uma solução de IPS. Ao receber requisições HTTP (porta 80/TCP), por exemplo, o Firewall da organização permite que o tráfego seja encaminhado, porém agora cabe ao sistema IPS analisar esse tráfego e, eventualmente, na presença de requisições maliciosas, tomar ações de prevenção. Além disso, na arquitetura apresentada na Figura 5.1, a comunicação entre diferentes segmentos de rede da organização também é inspecionada pelo IPS, prevenindo a propagação de atividade maliciosa na rede interna.

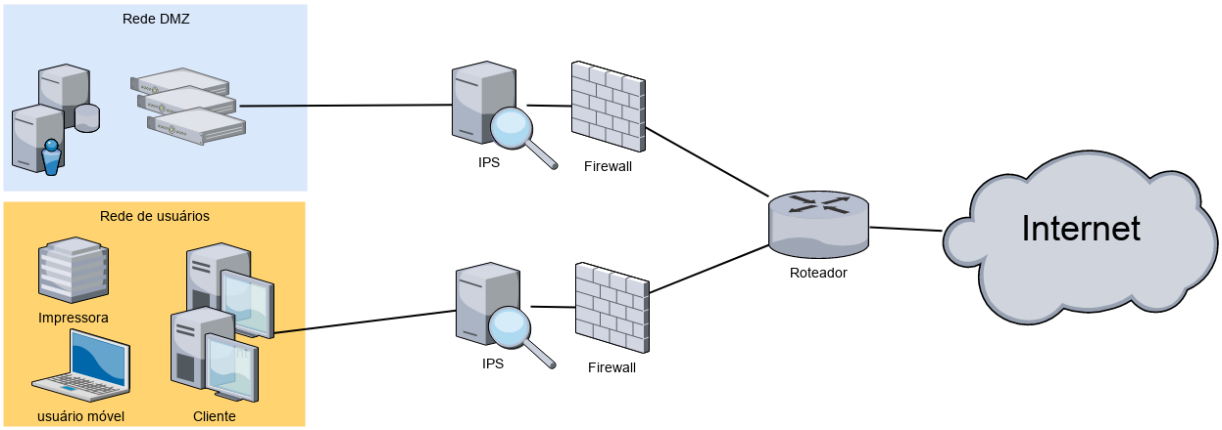


Figura 5.1 - Arquitetura com IPS inline na proteção da rede

É comum que a solução de detecção e prevenção de intrusos seja implantada em um mesmo sistema, levando o nome simplesmente de IPS. Em qualquer caso, esses sistemas são uma barreira importante de segurança para prevenir invasões na organização. Não obstante, dependendo do modelo de implantação que for adotado, alguns pontos de atenção devem ser analisados: 1) como esse sistema tem a capacidade de bloquear ataques, a própria segurança do IPS deve ser cuidadosamente avaliada para evitar comprometimento; 2) deve-se ter muito cuidado com falsos positivos e falsos negativos; 3) deve-se atentar para o desempenho do sistema, principalmente quando “inline”, para não impactar na qualidade da rede da organização; 4) as ações de contenção devem ser comunicadas dentro da organização.

A coleta de evidências constitui-se um importante requisito para auditorias futuras acerca das ações de mitigação de uma invasão. Esse processo é realizado através do registro nas trilhas de auditoria (logs) dos eventos de detecção e prevenção. Os logs geralmente são armazenados em formato SYSLOG, porém podem ser armazenados também em formato JSON ou até mesmo em bancos de dados SQL. Dessa maneira, o administrador da rede poderá não apenas tomar ações quanto ao ataque, mas também estará apto a responder questionamentos futuros quanto à ação executada. Por outro lado, essas evidências devem ser coletadas e armazenadas tendo em vista o respeito à privacidade do usuário.

5.2 Contenção de intrusos

A partir dos alarmes gerados na fase de detecção, o IPS executa ações de contenção para interromper o ataque e evitar maiores danos. Essas ações podem ser das mais variadas naturezas:

- Cancelamento da conexão em andamento (ex: envio de pacotes TCP RST);
- Bloqueio do host atacante através da configuração de regras de Firewall;
- Limitação de banda e requisições do atacante (*rate-limit*);
- Redirecionamento de tráfego para VLAN de quarentena para máquinas internas comprometidas;
- Redirecionamento do tráfego para sistemas de "*honeypot*" para estudar o ataque;
- Limpeza do tráfego removendo partes maliciosas do fluxo de dados;
- Dentre tantas outras possibilidades.

Em verdade, o conjunto de ações suportadas pelo IPS depende diretamente das tecnologias utilizadas (ex: Firewall, ferramentas de NAC - Network Access Control, scripts de bloqueio, etc) e do modelo de implantação adotado (ex: inline versus espelhado). No modelo de implantação inline, geralmente o próprio IPS é responsável pela execução das ações de contenção, portanto há uma flexibilidade maior pela adoção de tecnologias no próprio IPS para realizar os bloqueios. Por outro lado, no modelo de IPS espelhado o sistema depende da interação com outros elementos de rede na tomada da decisão.

Um exemplo desse cenário é ilustrado na Figura 5.2. Nessa figura uma máquina comprometida (ex: usuário clicou em um anexo infectado) realiza acesso a um IP malicioso (1) de servidor de Comando e Controle (servidor malicioso que é usado para controlar máquinas infectadas remotamente como se fossem zumbis). Em seguida, o sistema IPS espelhado identifica aquele tráfego anômalo (2) e notifica o Firewall (3) para redirecionar aquele tráfego ao servidor de quarentena. A partir daí, ao realizar qualquer outro tipo de acesso, a máquina ficará restrita ao ambiente de quarentena (4) até que seja efetuada uma análise com antivírus e antimalware para limpar a máquina.

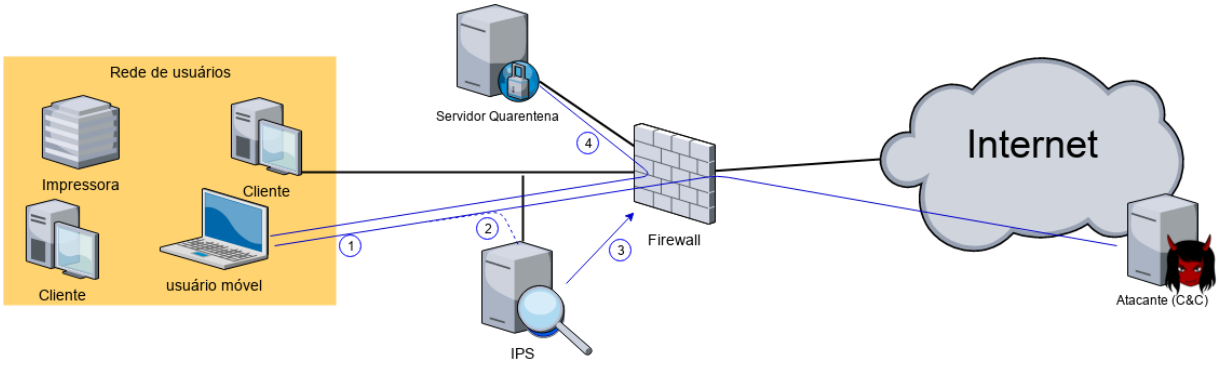


Figura 5.2 - Ilustração de sistema de IPS espelhado com contenção via quarentena.

A fim de suportar redirecionamento de tráfego para uma VLAN de quarentena, a solução de IPS deveria ser capaz de realizar modificações na camada de enlace do pacote ou aplicar alguma técnica de roteamento baseado em política. Em casos de IPS em modo espelhado, esses desafios são ainda maiores ao considerar que o elemento de rede que irá de fato realizar a contenção precisa ter algum suporte a essas tecnologias (ex: *MAC based VLAN*, *Policy Based Routing*, etc), além de disponibilizar um mecanismo para configuração remota (ex: SNMP, SSH, NETCONF, API REST, etc).

5.3 Uso de SDN para execução de ações de contenção

O uso de SDN e Openflow nesse contexto de contenção de ataques do IPS pode potencializar o conjunto de contramedidas adotadas, principalmente através da flexibilidade e programabilidade que são incorporadas. Além disso, Openflow fornece uma API padronizada para comunicação com os switches, o que pode impulsionar estratégias que visam bloquear os ataques mais próximos de sua origem na rede. Diversas aplicações SDN fornecem uma API para integração de sistemas, geralmente através de REST. As APIs de comunicação com switches, também conhecida como API sul, e API de comunicação com aplicações SDN, conhecida como API norte, pode ser visualizada conforme ilustrado na Figura 5.3.

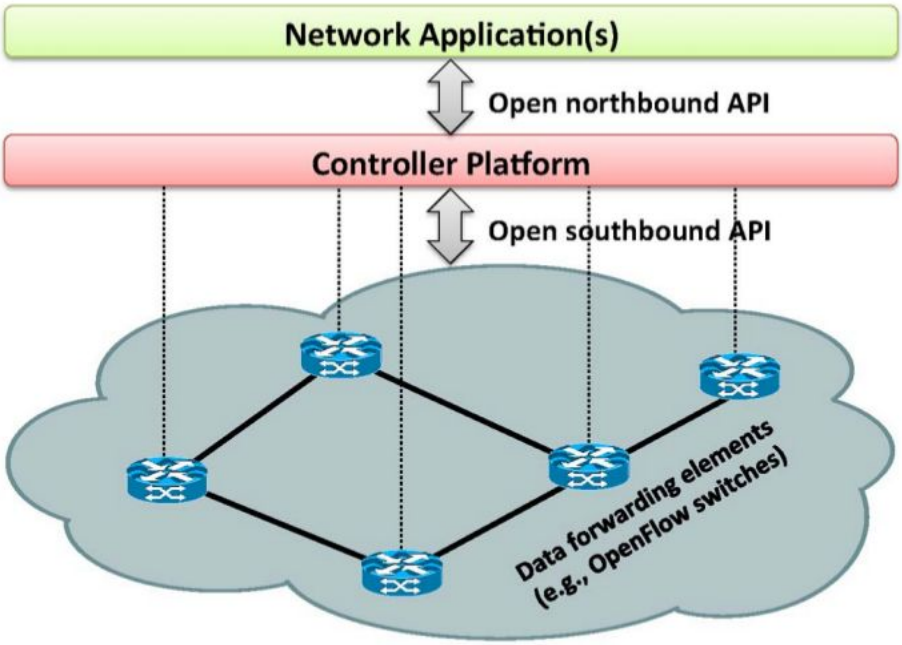


Figura 5.3 - Arquitetura simplificada de SDN e APIs norte e sul [Kreutz et al., 2015]

O protocolo Openflow define um conjunto de ações que podem ser tomadas para determinado fluxo de pacotes. Essas ações dependem da versão do protocolo suportada pelo switch e dependem do fabricante ou tipo de switch Openflow em questão (muitas ações são consideradas opcionais na especificação do protocolo). A versão 1.0 do protocolo Openflow, versão disponível no FIBRE e mais amplamente usada nas organizações, permite executar ações em relação à interfaces físicas, filas e até mesmo protocolos da camada de transporte (L4). É importante notar que ações em protocolos como Ethernet, IPv4, TCP e UDP são opcionais, o que limita de alguma maneira a integração de SDN com IPS. O Quadro 5.1 apresenta um resumo das principais ações do Openflow 1.0.

Quadro 5.1. Principais ações do Openflow 1.0 e comandos do Open vSwitch

Protocolo/Tipo	Comportamento	Alvo
<vazio>	Descarte	Descartar o pacote
Port	Encaminha	(output:port), onde *port* pode ser: **PORT-ID**: encaminha para porta específica **ALL**: encaminha para todas as portas exceto porta de origem

		INGRESS: envia para porta de entrada **CONTROLLER**: envia para o controlador **TABLE**: re-injeta o pacote para processamento novamente **LOCAL**: envia para o S.O. **FLOOD**: envia para todas as portas exceto a porta de entrada **NORMAL**: reprocessa o pacote na pilha de rede convencional
Queue	Modifica	Queue-ID - modifica o pacote de fila (set_queue:queue-id)
Ethernet	Modifica	MAC de origem (mod_dl_src:mac) MAC de destino (mod_dl_dst:mac) VLAN ID (mod_vlan_vid:vlan_vid) Prioridade VLAN (mod_vlan_pcp:vlan_pcp)
	Strip	VLAN ID - Remove a tag de vlan (strip_vlan)
IPv4	Modifica	IP de origem (mod_nw_src:ip) IP de destino (mod_nw_dst:ip) Tipo de serviço ToS (mod_nw_tos:tos)
TCP/UDP	Modifica	Porta de origem (mod_tp_src:port) Porta de destino (mod_tp_dst:port)

A partir desse conjunto de ações é possível implantar diferentes mecanismos de contenção no Sistema de Prevenção de Intrusos, alguns exemplos são:

- Bloqueio de host: para realizar o bloqueio de um host através de regra Openflow, a aplicação pode enviar uma mensagem de *FlowMod* (modificação de fluxo) com o parâmetro *actions* vazio;
- VLAN de quarentena: para realizar a contenção de um host por meio de um isolamento de quarentena via regra Openflow, a aplicação pode enviar uma mensagem de *FlowMod* (modificação e fluxo) com o parâmetro *actions* contendo o comando mod_vlan_vid:vlan_vid;
- Redirecionamento de tráfego: para realizar o redirecionamento de um host via regra Openflow, a aplicação pode enviar uma mensagem de *FlowMod* (modificação e fluxo)

com o parâmetro *actions* contendo o comando mod_nw_dst:ip (redirecionamento em em camada 3) ou mod_dl_dst:mac (para redirecionamento em camada 2).

De toda maneira, a execução de ações de contenção através de regras Openflow apresenta importantes desafios de implantação, a saber: como a tabela de fluxos não armazena estado, o controlador SDN deve dinamicamente mapear esses estados na sua tabela; a tomada de ações através do envio de pacotes de resposta (ex: TCP RST) depende de Packet Out pelo controlador, o que pode degradar o desempenho; Openflow 1.0 tem um conjunto restrito de campos de casamento de ações, o que limita, por exemplo a aplicação de técnicas de rate-limit; dentre outros.

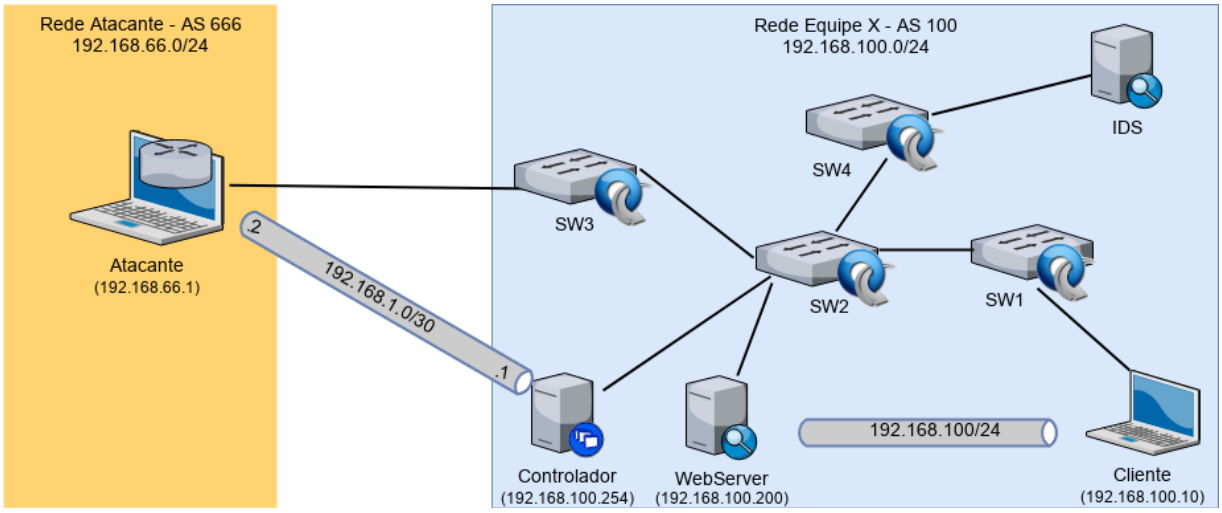
O roteiro de prática deste capítulo apresenta dois exemplos para realizar a contenção de hosts.

5.4 Exercícios de Fixação

1. Quais os tipos de ação de prevenção que podem ser adotadas pelo IPS?
2. Considerando um sistema IDS espelhado, quais os desafios para torná-lo um IPS?
3. Como o Controlador SDN pode implantar uma técnica de contenção baseada em quarentena?
4. Como o Controlador SDN pode implantar uma técnica de contenção baseada em cancelamento da conexão TCP?

5.5 Roteiro de laboratório

Neste laboratório será realizado a configuração de ações de contenção através do controlador SDN a partir dos alertas que são identificados pelo IDS. As ações de contenção ocorrerão de forma diferenciada para hosts intrusos internos e externos: para hosts externos a contenção se dará pelo simples bloqueio, ao passo que para hosts internos a contenção será realizada através de quarentena do host. A topologia utilizada neste laboratório é a mesma anterior, conforme Figura 5.4.



5.4. Topologia proposta para os experimentos da Oficina.

5.5.1 Configurando o script de contenção no IDS

Nesta prática o objetivo é instalar e configurar o Guardian, uma ferramenta que simplesmente monitora os eventos de alertas do IDS e executa ações configuradas, para conter automaticamente os hosts relacionados com atividades maliciosas na rede.

Esta prática pressupõe que o roteiro anterior do capítulo tenha sido executado com sucesso. Portanto, caso tenha desligado o ambiente ao final da prática anterior, é necessário religar o controlador Ryu. Ele irá recarregar as configurações que foram realizadas anteriormente a partir do arquivo **`sdn-ips-config.json`** na mesma pasta da aplicação.

1) Na máquina IDS, baixe o “Guardian Active Response” conforme abaixo:

```
su
wget https://goo.gl/ansjP8 -O guardian-1.7.tar.gz
tar -xzf guardian-1.7.tar.gz
cd guardian-1.7/
```

2) Copie o arquivo de configuração do Guardian para o diretório /etc e edite o arquivo, ajustando os parâmetros AlertFile e RemoteController para indicar o arquivo de alertas do Suricata e o IP da máquina Controlador (<IP-CONTROLADOR>, conforme saída do comando

“ifconfig eth0” no Controlador ou é possível ver também via interface do OCF), respectivamente:

```
cp guardian.conf /etc/
sed -i 's@/var/adm/secure@/var/log/suricata/fast.log@g' /etc/guardian.conf
sed -i 's@X.X.X.X@<IP-CONTROLADOR>@g' /etc/guardian.conf
```

3) Copie o arquivo guardian.pl para o diretório /usr/local/bin e copie os scripts de bloqueio e desbloqueio referentes à aplicação SDN-IPS para o mesmo diretório:

```
cp guardian.pl /usr/local/bin/
cp scripts/sdnips_block.sh /usr/local/bin/guardian_block.sh
cp scripts/sdnips_unblock.sh /usr/local/bin/guardian_unblock.sh
```

4) Antes de iniciar o Guardian vamos zerar as notificações do Suricata para evitar o bloqueio ocasionado pelo teste da seção anterior e zerar os logs do Guardian:

```
echo > /var/log/suricata/fast.log
echo > /var/log/guardian.log
/etc/init.d/suricata restart
```

5) Execute o Guardian com o seguinte comando:

```
/usr/local/bin/guardian.pl -c /etc/guardian.conf
```

5.5.2 Teste com bloqueio de host externo

Nesta prática vamos realizar um ataque a partir da máquina Atacante contra a máquina WebServer e observar que o IDS irá detectar o ataque e requisitar o bloqueio ao Controlador.

1) Na máquina Atacante, vamos realizar um teste de ataque de Negação de Serviço (DoS) do tipo TCP SYNFLOOD utilizando o comando hping3:

```
su
hping3 --fast -S -p 80 192.168.100.200
```

2) Na máquina IDS, observe os logs do Guardian que o ataque foi identificado e bloqueado:

```
tail /var/log/guardian.log
```

Deverá ser exibida uma mensagem como mostrado abaixo:

```
root@IDS:~/guardian-1.7# tail /var/log/guardian.log

Guardian process id 565
Thu Nov 30 00:53:10 2017: 192.168.66.1  [1:10001:1] Possible TCP Syn Flood DoS
Running '/usr/local/bin/guardian_block.sh 192.168.66.1 eth0'
```

3) Observe no console do Controlador os logs da aplicação SDN-IPS que o host foi bloqueado:

```
(1482) accepted ('10.144.12.56', 60956)
==> contention_block ipaddr=192.168.66.1 in all switches
10.144.12.56 - - [30/Nov/2017 01:15:32] "POST /sdnips/contention/block HTTP/1.1" 200 119 0.008405
```

4) Finalmente, de volta à máquina Atacante observe que não é possível mais realizar acesso ao servidor WebServer:

```
wget http://192.168.100.200
```

A saída esperada é erro de Timeout, uma vez que a máquina foi bloqueada:

```
root@Atacante:~# wget -T 3 http://192.168.100.200
converted 'http://192.168.100.200' (ANSI_X3.4-1968) -> 'http://192.168.100.200' (UTF-8)
--2017-11-30 01:02:19--  http://192.168.100.200/
Connecting to 192.168.100.200:80... failed: Connection timed out.
Retrying.

--2017-11-30 01:02:23--  (try: 2)  http://192.168.100.200/
Connecting to 192.168.100.200:80... failed: Connection timed out.
Retrying.
```

5.5.3 Teste com quarentena de host interno

Nesta prática vamos realizar um acesso malicioso a partir da máquina Cliente contra um IP de C&C e observar que o IDS irá detectar este comportamento malicioso e requisitar a quarentena ao Controlador.

1) Na máquina Cliente, vamos simular um acesso a IP malicioso de C&C (servidor de *Command and Control*). Para isso, acesse o site do Tracker do Trojan Feodo (ou qualquer outro da lista da emergint-threats botcc), mantido pelo time de segurança abuse.ch através do site https://feodotracker.abuse.ch/, escolha algum IP que esteja online de C&C para simular o acesso. A partir daí vamos rotear esse IP através da rede do AS100 e simular um acesso. Para isso execute o seguinte comando (atente-se para alterar o <IP-CnC> para o IP escolhido):

```
route add -host <IP-CnC> gw 192.168.100.254
wget -q -O - http://<IP-CnC>/
```

Observe que a requisição será redirecionada automaticamente para o host WebServer e você receberá como retorno a mensagem:

```
root@Cliente:~# wget -q -O - http://95.85.19.195/
<h1>SDN-IPS: Sua maquina foi identificada como possivelmente infectada! Procure o departamento de TI da organizacao!</h1>
root@Cliente:~#
```

3) Observe no console do Controlador os logs da aplicação SDN-IPS que o host foi bloqueado:

```
(1414) accepted ('10.144.12.56', 60955)
10.144.12.56 - - [30/Nov/2017 01:05:16] "POST /sdnips/contention/quarantine HTTP/1.1" 200 119 0.008196
==> create contention_quarantine_redirect in dpid=00000cc47a5e9894 src=192.168.100.10 dst=95.85.19.195 redirect_to=192.168
.100.200
```

Ao final deste experimento, o aluno deve ter sido capaz de criar regras para contenção dos ataques e verificar a atuação dessas regras aplicadas a diferentes contextos (interno e externo à organização).