PacketFence – versão 3.0.3

Guia de Administração

Versão 3.0.3 – Novembro 2011

Sumário

Capítulo 1

Sobre este Guia

Este guia irá conduzi-lo através da instalação e do dia a dia de administração da solução PacketFence.

As instruções são baseadas na versão 3.0.3 do PacketFence

A última versão deste guia está disponível em http://www.packetfence.org/documentation/

Outras fontes de informação

Guia de Configuração de Dispositivos de Rede - Switch, controladores e configuração de Access Points.

Guia do Desenvolvedor – Personalização do Captive Portal, VLAN personalização de gerência e instruções para suportar novo hardware.

Para uma lista de mudanças notáveis desde a última versão ver o arquivo `NEWS`.

Para uma lista de alterações relacionadas com a compatibilidade e notas sobre a atualização ver o arquivo `UPGRADE`.

Para mais detalhes e mudanças visíveis no desenvolvimento ver o arquivo `ChangeLog`.

Esses arquivos estão incluídos no pacote e tarballs de lançamento

Capítulo 2

Introdução

PacketFence é totalmente suportado, confiável, gratuito e um sistema Open Source de Controle de Acesso à Rede (NAC). Impulsionar um conjunto de características impressionantes, incluindo um Captive Portal para registro e re-mediação, gerenciamento centralizado com fio e sem-fio, suporte 802.1x, isolamento de dispositivos problemáticos na camada 2, integração com o IDS Snort e do scanner de vulnerabilidade Nessus; PacketFence pode ser usado efetivamente para redes seguras - de pequena a grandes redes heterogêneas.

Características

- Fora de banda (execução de VLAN)

  PacketFence é completamente uma operação fora de banda que permite a solução, a escala geográfica e ser mais resistente às falhas.

- Em Banda (Aplicação Inline)

  PacketFence pode também ser configurado para ser em banda, especialmente quando o usuário tem switches não gerenciáveis ou pontos de acesso. PacketFence também trabalha tanto com à VLAN e aplicação Inline ativada para a máxima escalabilidade e segurança quando permite ao hardware mais antigos ainda serem hardwares a serem segura utilizando a aplicação Inline.

- Suporte a Voz sobre IP (VoIP).

  Também chamado de Telefonia IP (IPT), VoIP é totalmente suportada (mesmo em ambientes heterogêneos) para mútiplos fornecedores de switch (Cisco, Edge-Core, HP, LinkSys, Nortel Networks e muito mais).

- 802.1X

  802.1X sem fio e com fio é suportado através de um módulo FreeRADIUS.

- Integração Wireless

  PacketFence integra perfeitamente com redes sem fio através de um módulo FreeRADIUS. Isso permite ao usuário proteger suas redes sem fio e com fio da mesma forma usando o banco de dados de usuário e usando o mesmo no Captive Portal,

proporcionando uma experiência consistente. Mistura de fornecedores de pontos de acesso (AP) e controladores sem fio é suportado.

- Registro

PacketFence suporta um mecanismo de registro opcional semelhante as soluções de Captive Portal. Ao contrário do que soluções captive portal, o PacketFence lembra usuários previamente cadastrados e automaticamente dar-lhes acesso sem outra autenticação. Claro, isso é configurável. Uma Política de Utilização aceitável pode ser especificada de tal forma que os usuários não podem permitir o acesso à rede sem antes aceitá-lo.

- Detecção de atividades anormal de rede.

Atividades anormal de rede (vírus de computador, worms, spyware, tráfego negado por políticas estabelecidas, etc.) podem ser detectadas usando sensores Snort locais e remotos. Além de detecção simples, PacketFence possui sua própria camada de alerta e mecanismo de repressão em cada tipo de alerta. Um conjunto de ações configuráveis para cada violação está disponível para administradores.

- Varredura de vulnerabilidade Pró-Ativa

Nessus varreduras de vulnerabilidade podem ser executadas no momento do registro, programado ou numa base ad-hoc. PacketFence correlaciona a vulnerabilidade Nessus ID de cada varredura na configuração de violação, retornando páginas web de conteúdo específico sobre o qual a vulnerabilidade do host pode ter.

- Isolamento de dispositivos problemáticos

PacketFence suporta várias técnicas de isolamento, incluindo isolamento de VLAN com suporte VoIP (mesmo em ambientes heterogêneos) para múltiplos fornecedores de switches.

- Re-mediação através de um Captive Portal

Uma vez preso, todo o tráfego da rede é finalizado pelo sistema PacketFence. Com base no estado atual do nó (não registrado, violação, etc) o usuário é redirecionado para a URL apropriada. No caso de uma violação, o usuário será apresentado com às instruções para a situação em particular dele/dela, reduzindo a intervenção do serviço de ajuda.

- Linha de comando e gerenciamento baseado na Web

Interfaces baseada na Web e linha de comando para todas as tarefas de gerenciamento.

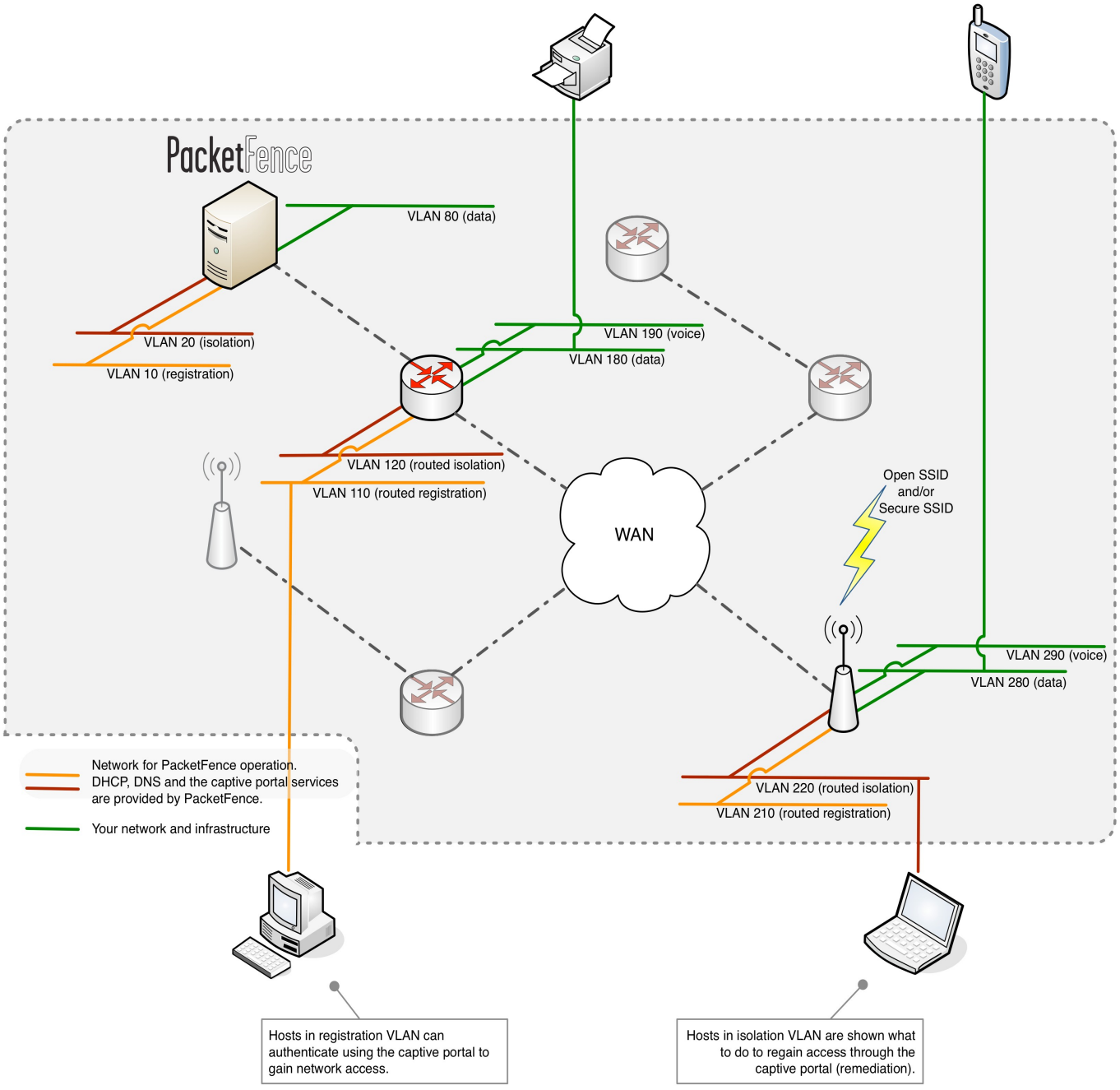
- Acesso a Visitantes

PacketFence suporta uma VLAN especial para convidado fora da caixa. Configurar sua

rede para que a VLAN de convidado só vai para a Internet, a VLAN de registro e captive portal são os componentes usados para explicar aos convidados como registrar para o acesso e como funciona o seu acesso. Isso é geralmente marcado pela organização que oferece o acesso. Vários meios de registro de convidado são possíveis. PacketFence também suporta acesso de convidado por criações e importações.

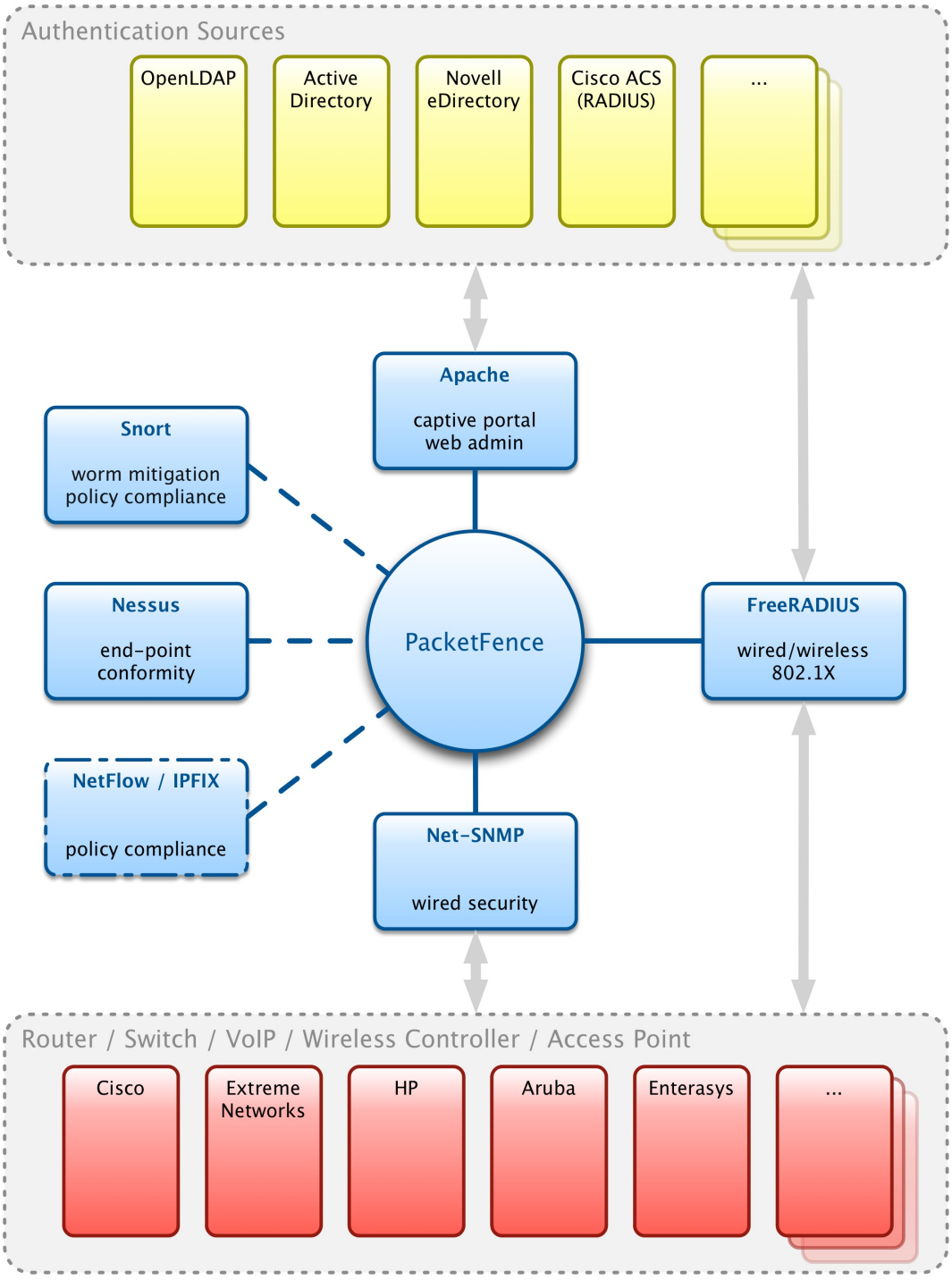
PacketFence é desenvolvido por uma comunidade de desenvolvedores localizados principalmente na América do Norte. Mais informações podem ser encontradas em http://www.packetfence.org

Integração de Rede



A aplicação da VLAN é demonstrado na figura do diagrama acima. A aplicação Inline deve ser considerada como uma rede simples onde o PacketFence atua como um firewall / gateway.

Componentes



Requisitos de Sistema

Suposições

PacketFence reutiliza muitos componentes em uma infraestrutura. Assim, exige o seguinte:

- Servidor de Banco de Dados (MySQL)
- Servidor Web (Apache)

Dependendo da configuração, o usuário pode ter de instalar componentes adicionais como:

- Servidor DHCP (ISC DHCP)
- Servidor DNS (BIND)
- Servidor RADIUS (FreeRADIUS)
- NIDS (Snort)

Neste guia, partimos do princípio de que todos os componentes estão em execução no mesmo servidor (ex., "`localhost`" ou "`127.0.0.1`") que o PacketFence será instalado.

Uma boa compreensão daqueles componentes e GNU/Linux é necessária para instalar o PacketFence. Se o usuário faltar alguns desses componentes necessários, por favor, consulte a documentação apropriada e prossiga com a instalação destes requisitos antes de continuar com este guia.

A tabela, a seguir, fornece recomendações para os componentes necessários, junto com números de versão:

Servidor MySQL	MySQL 4.1 ou 5.1
Servidor Web	Apache 2.2
Servidor DHCP	DHCP 3
Servidor DNS	BIND 9
Servidor RADIUS	FreeRADIUS 2
Snort	Snort 2.8 ou 2.9

Versões mais recentes dos softwares mencionados acima também podem ser usadas.

Requisitos mínimos de hardware

A tabela, a seguir, fornece recomendações para o Servidor e Desktops:

Servidor	▪ Intel ou AMD CPU 3 GHz ▪ 2048 MB de RAM ▪ 20 GB de espaço em disco (RAID 1 recomendado) ▪ 1 Placa de rede ■ + 1 para alta disponibilidade ■ + 1 para detecção de intrusão

Capítulo 3

Requisitos do sistema operacional

PacketFence suporta os seguintes sistemas operacionais nas arquiteturas i386 ou x86_64:

- Red Hat Enterprise Linux 5.x/6.x Server
- Community ENTerprise Operating System (CentOS) 5.x/6.x

Certifique-se de que o usuário pode instalar pacotes adicionais a partir de sua distribuição padrão. Por exemplo, se o usuário estiver usando o Red Hat Enterprise Linux, o usuário tem de ser inscrito no Red Hat Network antes de continuar com a instalação do software PacketFence.

Outras distribuições, tais como, Debian, Fedora e Gentoo, são conhecidas para trabalhar, mas este documento não irá cobri-las.

Serviços de Inicialização

PacketFence cuida do funcionamento e operação dos seguintes serviços:

- Servidor Web (httpd)
- Servidor DHCP (dhcpd)
- Servidor DNS (named)
- Servidor FreeRADIUS (radiusd)
- Snort Network IDS (snort)
- Firewall (iptables)

Certifique-se de que todos os outros serviços são automaticamente iniciados pelo seu sistema operacional

Capítulo 4

Instalação

Esta seção irá guiá-lo através da instalação do PacketFence juntamente com suas dependências.

Instalação do Sistema Operacional

Instalar sua distribuição com a instalação mínima e nenhum pacote adicional. Então:

- Ative o Firewall
- Desative o SELinux

Certifique-se de que seu sistema está atualizado e seu banco de dados está atualizado:

```
yum update
```

RHEL 5.x / CentOS 5.x

Algumas dependências do PacketFence estão disponíveis através do repositório Repoforge (http://repoforge.org/) então o usuário precisa configurar o YUM para usá-lo.

Em seguida, instale a última versão do pacote RPMForge para sua arquitetura (http://pkgs.repoforge.org/rpmforge-release/): Por exemplo (i386):

```
wget http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.2-
2.el5.rf.i386.rpm
rpm -i rpmforge-release-0.5.2-2.el5.rf.i386.rpm
```

Desabilitar o repositório por padrão. No arquivo /etc/yum.repos.d/rpmforge.repo, altere sob a seção rpmforge para 0:

```
enabled = 0
```

Então instale o repositório EPEL (http://fedoraproject.org/wiki/EPEL/FAQ). Fazer assim, simplesmente pegue o último rpm EPEL (versão 5.4 no momento deste lançamento), e instale-o :

```
wget http://download.fedoraproject.org/pub/epel/5/i386/epel-release-5-4.noarch.rpm
rpm -i epel-release-5-4.noarch.rpm
```

RHEL 6.x / CentOS 6.x

Algumas dependências do PacketFence estão disponíveis através do repositório Repoforge (http://repoforge.org/) então o usuário precisa configurar o YUM para usá-lo.

Em seguida, instale a última versão do pacote RPMForge para sua arquitetura (http://pkgs.repoforge.org/rpmforge-release/): Por exemplo (x86_64):

```
wget http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.2-2.el6.rf.x86_64.rpm
rpm -i rpmforge-release-0.5.2-2.el6.rf.x86_64.rpm
```

Desabilitar este repositório por padrão. No arquivo /etc/yum.repos.d/rpmforge.repo, altere sob a seção rpmforge para 0:

```
enabled = 0
```

Então instale o repositório EPEL (http://fedoraproject.org/wiki/EPEL/FAQ). Fazer assim, simplesmente pegue o último rpm EPEL (versão 6.5 no momento deste lançamento), e instale-o :

```
wget http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-5.noarch.rpm
rpm -i epel-release-6-5.noarch.rpm
```

RHEL 6.x

Usuários RedHat Enterprise Linux necessitam de um passo adicional na configuração. Se o usuário não estiver usando o Gerenciamento de Assinatura RHN da RedHat, o usuário precisa habilitar o o canal opcional executando o seguinte como root:

```
rhn-channel --add –channel=rhel-`uname -m`-server-optional-6
```

RedHat parece não fornecer um pacote `perl-Net-Telnet`. PacketFence precisa dele por isso, nós vamos instala-lo do repositório `rpmforge-extras` agora:

```
yum install perl-Net-Telnet --enablerepo=rpmforge-extras
```

Download de software

Começando com 1.8.5, PacketFence, agora é fornecido como um repositório RPM para RHEL / CentOS em vez de um arquivo RPM único.

Este repositório contém todas as dependências necessárias para instalar o PacketFence. Isto proporciona inúmeras vantagens:

- Instalação muito fácil
- Tudo é empacotado como RPM (sem problemas CPAN)
- Atualização fácil

Instalação de Software

Para usar o repositório, basta criar um arquivo chamado `/etc/yum.repos.d/PacketFence.repo` com o seguinte conteúdo:

```
[PacketFence]
name=PacketFence Repository
baseurl=http://inverse.ca/downloads/PacketFence/RHEL$releasever/$basearch
gpgcheck=0
enabled=0
```

Uma vez definido o repositório, o usuário pode instalar o PacketFence com todas as dependências necessárias aos serviços (DNS, servidor de banco de dados, servidor DHCP, servidor RADIUS) usando:

```
yum groupinstall --enablerepo=PacketFence,rpmforge Packetfence-complete
```

Ou, se preferir, para instalar somente o núcleo do PacketFence sem todos os serviços externos, o usuário pode usar:

```
yum install --enablerepo=PacketFence,rpmforge packetfence
```

Uma vez instalado, execute o instalador e siga as instruções:

```
/usr/local/pf/installer.pl
```

Uma vez completado, o PacketFence será totalmente instalado em seu servidor. Agora o usuário

está pronto para configurá-lo.

Configuração

Nesta seção, o usuário aprenderá como configurar o PacketFence. PacketFence usará MySQL, Apache, ISC DHCP, ISC DNS, iptables e FreeRADIUS Como mencionado anteriormente, assumimos que todos os componentes são executados no mesmo servidor em que o PacketFence está sendo instalado.

Primeiro Passo

Afim de começar corretamente a configuração do PacketFence, recomendamos executar o script de configuração localizado em`/usr/local/pf/configurator.pl`. Este script irá guiá-lo através do processo de criação de um arquivo de configuração de trabalho do PacketFence que seja adequado às suas necessidades.

O script irá dar-lhe caminhos diferentes para a configuração. Dependendo do que o usuário quer alcançar, responda às perguntas que lhe é apresentado. O script vai pedir mais algumas informações sobre sua infraestrutura de rede, como os servidores DNS e os servidores de endereços DHCP, etc.

Tenha em mente que a configuração resultante do PacketFence será localizado em `/usr/local/pf/conf/pf.conf` e `/usr/local/pf/conf/networks.conf` e ele sempre pode ser ajustado manualmente depois.

Interface de Administração baseada na Web

PacketFence fornece uma interface de administração baseada na web para fácil configuração e gerenciamento operacional. Afim de acessar a interface, o usuário precisa criar uma conta administrador e uma de serviços web.

O usuário precisa criptografar a nova senha no arquivo `admin.conf` com o `htpasswd`:

```
htpasswd -d /usr/local/pf/conf/admin.conf admin
```

Em seguida, digite a nova senha duas vezes.

Em seguida, novamente para webservice:

```
htpasswd -d /usr/local/pf/conf/admin.conf webservice
```

Em seguida, digite a nova senha duas vezes. Use uma senha forte. O usuário nunca terá que

entrar mais de uma vez.

Uma vez que o PacketFence é iniciado, a interface de administração está disponível em: https://<hostname> : 1443 /

Arquivo de configuração global (pf.conf)

O arquivo `/usr/local/pf/conf/pf.conf` contém a configuração geral do PacketFence. Por exemplo, este é o lugar onde informamos que o PacketFence trabalhará no modo de isolamento VLAN.

Todos os parâmetros padrões e suas descrições são armazenadas em `/usr/local/pf/conf/pf.conf.defaults`.

A fim de substituir um parâmetro padrão, defina-o e ajuste-o em `pf.conf`.

`/usr/local/pf/conf/documentation.conf` contém a lista completa de todos os parâmetros disponíveis.

Todos estes parâmetros também são acessíveis através da interface Web de Administração sob a guia Configuração.

Captive Portal

Parâmetros importantes a configurar a respeito do captive portal são os seguintes:

`redirecturl` em `[trapping]`

Para alguns navegadores, é preferível redirecionar o usuário para uma URL específica em vez da URL que o usuário originalmente pretendia visitar. Para estes navegadores, a URL definida em `redirectUrl` será a única na qual o usuário será redirecionado. Navegadores afetados são Firefox 3 e Firefox 4.

`network_detection_ip` em `[captive_portal]`

Este IP é usado como o servidor web que hospeda o `common/network-access-detection.gif` que é usado para detectar se o acesso à rede foi ativada. Não pode ser um nome de domínio, uma vez que é usado em registro ou quarentena no qual o DNS é rejeitado. É recomendado que o usuário permita que seus usuários cheguem ao seu servidor PacketFence e coloque o IP da sua LAN no PacketFence. Por padrão, nos faremos o web site deste PacketFence chegar como uma solução mais fácil e mais acessível.

Configuração do Apache

A configuração do PacketFence para o Apache está localizado em `/usr/local/pf/conf/httpd.conf`.

Após a instalação do PacketFence, um arquivo de configuração padrão é criado, que é adequado para a maioria das configurações. SSL é ativado por padrão para proteger o acesso.

Se o usuário usou o script installer.pl, o usuário deve ter certificados SSL auto-assinados em `/usr/local/pf/conf/ssl` (Server.key e server.crt). Estes certificados podem ser substituídos a

qualquer momento pelo seu terceiro ou certificado curinga existente sem problemas. Por favor, note que o CN (Common Name) deve ser o mesmo que o definido no arquivo de configuração do PacketFence (pf.conf).

SELinux

Mesmo que essa característica pode ser pretendida por algumas organizações, o PacketFence não será executado corretamente se o SELinux está definido para enforced. Você precisará desativá-lo explicitamente no arquivo em `/etc/selinux/config`.

Autenticação (arquivo simples, LDAP/AD, RADIUS)

PacketFence pode autenticar os usuários que registram os dispositivos através do portal captive usando um arquivo simples, um servidor LDAP (ou Active Directory) ou um servidor RADIUS.

Arquivo simples

Por padrão, o PacketFence olha para `/usr/local/pf/conf/user.conf` para encontrar os usuários autorizados a registrar dispositivos. Se o usuário quiser usar um arquivo diferente, edite `/usr/local/pf/conf/authentication/local.pm` e altere o seguinte parâmetro:

```
my $passwdFile = '/usr/local/pf/conf/user.conf';
```

O usuário precisa criptografar a senha de cada usuário com htpasswd assim:

```
htpasswd -d /usr/local/pf/conf/user.conf newuser
```

LDAP / Active Directory (AD)

Edite `/usr/local/pf/conf/authentication/ldap.pm` e faça as alterações necessárias para os seguintes parâmetros :

```
my $LDAPUserBase = "ou=People,dc=domain,dc=org";
my $LDAPUserKey = "uid";
my $LDAPUserScope = "one";
my $LDAPBindDN = "cn=ldapuser,dc=domain,dc=org";
```

```
my $LDAPBindPassword = "password";
my $LDAPServer = "127.0.0.1";
```

RADIUS

Edite `/usr/local/pf/conf/authentication/radius.pm` e faça as alterações necessárias para os seguintes parâmetros:

```
my $RadiusServer = 'localhost';
my $RadiusSecret = 'testing123';
```

Selecionando um Método de Autenticação

Para configurar a autenticação defina o `[registration].auth` em option `/usr/local/pf/conf/pf.conf`:

```
auth=local,ldap,radius
```

Se mais de um método são especificados, PF irá exibir uma lista suspensa para permitir aos usuários selecionar o método de autenticação preferido.

O nome do método de autenticação exibido no drop-down é controlado pela variável `$name` no módulo de autenticação (localizado em `conf/authentication/`). Sinta-se livre para modificar os nomes à medida das necessidades da sua organização.

Método de Autenticação Padrão

Método de autenticação selecionado como o padrão no portal captive no drop-down. Apenas útil se o usuário tiver mais de um método de autenticação (em registration.auth).

Definição dos dispositivos da Rede (switches.conf)

Esta seção se aplica apenas para a aplicação da VLAN. Usuários planejando fazer somente a aplicação Inline pode pular esta seção.

PacketFence precisa saber que switches, access points ou controladores que gerencia, seu tipo e con fguração. Todas essas informações são armazenadas em `/usr/local/pf/conf/switches.conf`. O usuário pode modificar a configuração diretamente no arquivo `switches.conf` ou o usuário pode fazê-lo no painel de Administração Web em Configuration -> Switches.

Estes arquivos contém uma seção padrão, incluindo:

- Lista de VLANs gerenciado pelo PacketFence

- ❑ Padrão SNMP de comunidades de leitura/gravação para os switches
- ❑ Modo de trabalho padrão (veja a nota sobre o modo de trabalho abaixo)

e a seção switch para cada switch (gerenciado pelo PacketFence), incluindo:

- ❑ Switch IP
- ❑ Switch fornecedor/tipo
- ❑ Portas de switch uplink (troncos e portas não gerenciadas)
- ❑ por switch redefinição de vlans (se necessário)

Modos de trabalho

Existem três diferentes modos de trabalho:

- ❑ Testes: pfsetvlan escreve nos arquivos de log o que faria normalmente, mas não faz nada.
- ❑ Registro: pfsetvlan automaticamente registra todos os endereços MAC visto nas portas do switch. Como em modo de teste, nenhuma alteração VLAN foi realizada.
- ❑ Produção: pfsetvlan envia o SNMP para escrever a mudança de VLAN nas portas do switch.

SNMP v1, v2c e v3

PacketFence usa SNMP para comunicar com a maioria dos switches. Iniciando com 1.8, o PacketFence agora suporta SNMP v3. Você pode usar SNMP v3 para comunicação em ambas as direções: do switch para o PacketFence e do PacketFence para o switch.

De PacketFence para um switch

Editar o arquivo de configuração switch (`/usr/local/pf/conf/switches.conf`) e definir os seguintes parâmetros:

```
SNMPVersion = 3
SNMPUserNameRead = readUser
SNMPAuthProtocolRead = MD5
SNMPAuthPasswordRead = authpwdread
SNMPPrivProtocolRead = AES
SNMPPrivPasswordRead = privpwdread
SNMPUserNameWrite = writeUser
SNMPAuthProtocolWrite = MD5
SNMPAuthPasswordWrite = authpwdwrite
SNMPPrivProtocolWrite = AES
```

```
SNMPPrivPasswordWrite = privpwdwrite
```

De um switch para o PacketFence

Editar o arquivo de configuração switch (`/usr/local/pf/conf/switches.conf`) e definir os seguintes parâmetros:

```
SNMPVersionTrap = 3
SNMPUserNameTrap = readUser
SNMPAuthProtocolTrap = MD5
SNMPAuthPasswordTrap = authpwdread
SNMPPrivProtocolTrap = AES
SNMPPrivPasswordTrap = privpwdread
```

Configuração do Switch

Aqui está um exemplo de configuração do switch de forma a permitir SNMP v3 em ambas as direções em um Switch Cisco.

```
snmp-server engineID local AA5ED139B81D4A328D18ACD1
snmp-server group readGroup v3 priv
snmp-server group writeGroup v3 priv read v1default write v1default
snmp-server user readUser readGroup v3 auth md5 authpwdread priv aes 128
privpwdread
snmp-server user writeUser writeGroup v3 auth md5 authpwdwrite priv aes
128 privpwdwrite
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.0.50 version 3 priv readUser  port-security
```

Interface de linha de comando: Telnet e SSH

PackeFence precisa, às vezes, estabelecer uma sessão de linha de comando interativa com um switch. Isto pode ser feito usando Telnet. Iniciando com 1.8, agora o usuário pode usar SSH. A fim de fazê-lo, edite o arquivo de configuração switch (`/usr/local/pf/conf/switches.conf`) e definir os seguintes parâmetros:

```
cliTransport = SSH (ou Telnet)
cliUser = admin
```

```
cliPwd = admin_pwd
cliEnablePwd =
```

Também pode ser feito através da interface de administração Web em Configuration -> Switches.

Interface de Serviços Web

PackeFence, às vezes, precisa estabelecer um diálogo com capacidades de serviços da Web de um switch. A fim de fazê-lo, edite o arquivo de configuração switch (`/usr/local/pf/conf/switches.conf`) e definir os seguintes parâmetros:

```
wsTransport = http (ou https)
wsUser = admin
wsPwd = admin_pwd
```

Nota: a partir do PacketFence 1.9.1 poucos switches requerem configuração de Serviços Web, a fim de trabalhar. Também pode ser feito através da interface de administração Web em Configuration -> Switches.

Radius Secret

Mecanismo de autenticação para alguns, tais como, 802.1X ou autenticação MAC, o servidor RADIUS precisa ter o dispositivo de rede em sua lista de clientes A partir do PacketFence 3.0, que agora usa um servidor de banco de dados para armazenar as informações do cliente RADIUS. A fim de fazê-lo, edite o arquivo de configuração switch (`/usr/local/pf/conf/switches.conf`) e definir os seguintes parâmetros:

```
radiusSecret= secretPassPhrase
```

Atribuição da VLAN padrão

Esta seção se aplica apenas para a aplicação da VLAN. Usuários planejando fazer somente a aplicação Inline pode pular esta seção.

A técnica padrão de atribuição de VLAN usados em PacketFence é uma por switch. O padrão correto de VLAN para dado MAC é o `normalVlan` variável do switch onde o MAC está ligado ou a `[default]normalVlan` se o switch não especificar um `normalVlan`.

Isto permite que o usuário faça fácil segmentação de VLAN por construção.

Se precisar de mais flexibilidade (por SSID, por categoria de nó, etc) dar uma olhada no "eu preciso de mais flexível atribuição de VLAN" no item Recursos avançados.

Capítulo 5

Configuração da aplicação Inline

Esta seção se aplica apenas para a aplicação Inline. Usuários planejando fazer somente a aplicação de VLAN pode pular esta seção.

Introduzido em PacketFence 3.0, a aplicação Inliine é um método muito conveniente de realizar controle de acesso em hardware de rede mais antigo que não é capaz de fazer aplicação de VLAN ou que não é compatível com PacketFence. Esta técnica é abordada em detalhes na seção "Introdução técnica à aplicação Inline".

Um parâmetro importante da configuração a ter em mente é que quando configurando uma aplicação Inline alcançados pelos usuários deve ser a atual produção do servidor DNS. A seção seguinte mostra ao usuário como configurar apropriada Inline e é lá que o usuário deve se referir a produção apropriada do DNS.

Uma vez que somos incapazes de prever se o usuário terá controle sobre o seu DNS ou não, a técnica de redirecionamento padrão se baseia no endereço IP em vez de DNS. Isso significa que o seu certificado SSL irá gerar um erro quando apresentado ao usuário (o seu domínio não corresponde ao endereço IP do portal). Por causa disso, nós removemos suporte HTTPS obrigatório a partir do portal captive Inline no modo de redirecionamento de IP. Infelizmente, tivemos de fazer isso para tornar o modo Inline o mais simples possível. Essa limitação pode ser removida em uma versão futura.

Para remover essa limitação, se o usuário tem controle sobre o seu DNS, adicione uma entrada correspondente `hostname.domain` para o IP na interface de Inline do PacketFence. Em seguida, defina o parâmetro `inline.portal_redirect` para `dns`. Desta forma, o redirecionamento será baseado em SSL e o usuário não terá erros de certificado, se seu certificado CN está correspondendo plenamente com o PacketFence hostname totalmente qualificado.

Em resumo:

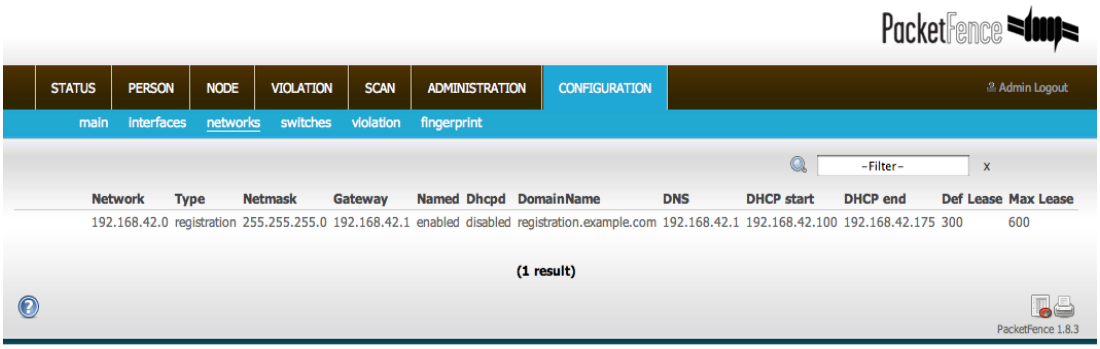
- `portal_redirect=ip` – padrão, nenhum HTTPS, nenhuma necessidade de modificar o DNS
- `portal_redirect=dns` – precisa ser atualizado o seu DNS, o portal estará em HTTPS

Configuração DHCP e Servidor DNS (networks.conf)

PacketFence gera automaticamente o DHCP e os arquivos de configuração do DNS para Registro e isolamento de VLANs. Isto é feito ao executar o script configurador (veja a Seção Geral de Configuração).

O registo e Isolamento da informação de redes estão acessíveis através da GUI em

Administration -> Networks:



- network: sub-rede
- netmask: Máscara de rede
- gateway: endereço IP PacketFence nesta rede
- next_hop: usado somente com redes roteadas; o endereço IP do roteador na rede (Isto é usado para criar rotas estáticas para as redes roteadas). Veja a Seção de redes Roteadas)
- domain-name: nome DNS
- dns: PacketFence endereço IP nesta rede
- dhcp_start: iniciando endereços IP do escopo DHCP
- dhcp_end: terminando endereços IP do escopo DHCP
- dhcp_default_lease_time: tempo padrão de concessão do DHCP
- dhcp_max_lease_time: tempo máximo de concessão do DHCP
- type: vlan-registration ou vlan-isolation ou inline
- named: PacketFence é o DNS para essa rede? (Enabled/Disabled) configurá-lo para habilitadas menos no tipo Inline onde deve ser desativado
- dhcpd: PacketFence é o servidor DHCP para essa rede? (Enabled/Disabled) defini-lo para enabled

Ao iniciar o PacketFence gera os arquivos de configuração do DHCP através da leitura das informações fornecidas em `networks.conf`:

O arquivo de configuração do DHCP é gerado para `var/conf/dhcpd.conf` usando `conf/dhcpd.conf` como um modelo.

Os arquivos de configuração de DNS são gerados desta forma:

- `var/conf/named.conf` gerados a partir de `conf/named.conf`
- `var/named/named-registration.ca` gerados a partir de `conf/named-registration.ca`
- `var/named/named-isolation.ca` gerados a partir de `conf/named-isolation.ca`

Desde o PacketFence 3.0, os arquivos de zona DNS são preenchidas automaticamente. Simplesmente assegurar que as informações estão nos arquivos de configuração gerados

(`var/conf/named/named-registration.ca` e `var/conf/named/named-isolation.ca`)

Acesso à Produção DHCP

A fim de realizar todas as suas funções de controle de acesso, o PacketFence precisa ser capaz de mapear endereços MAC em endereços IP.

Para todas as redes/VLANs na qual o usuário deseja o PacketFence tenha a capacidade de isolar um nó ou ter informações sobre IP dos nós, o usuário vai precisar executar **uma** das técnicas abaixo.

Note também que esta não precisa ser feito para o registro, isolamento de VLANs e interfaces Inline, desde que o PacketFence atua como o servidor de DHCP nestas redes.

Ajudantes IP (recomendado)

Se o usuário já estiver usando ajudantes IP para a sua produção em DHCP, em sua produção de VLANs esta aproximação é a mais simples e a única que trabalha melhor.

Adicione o endereço IP do gerente PacketFence como o último `ip helper-address` na declaração. Neste ponto, o PacketFence receberá uma cópia de todos os pedidos DHCP para essa VLAN e registrará o IP que foi distribuído para o nó usando um `pfdhcplistener` daemon.

Certifique-se de que nenhum servidor DHCP está executando na interface na qual o usuário está enviando os pedidos, senão o PacketFence pode tentar responder às solicitações de DHCP, o que seria uma coisa ruim.

Obter uma cópia do tráfego DHCP

Obter uma cópia de todos os tráfegos DHCP para uma interface física dedicada no servidor PacketFence e executar `pfdhcplistener` nessa interface. Envolverá configurar o switch para executar adequadamente espelhamento de porta (extensão de rede aka) e adicionando em PacketFence a declaração de interface adequada ao nível do sistema operacional e em `pf.conf`.

`/etc/sysconfig/network-scripts/ifcfg-eth1`:

```
DEVICE=eth2
ONBOOT=yes
BOOTPROTO=none
```

Adicionar ao `pf.conf`: (O IP não são importantes estão lá somente assim que o PacketFence vai começar)

```
[interface eth2]
```

```
mask=255.255.255.0
type=dhcp-listener
gateway=192.168.1.5
ip=192.168.1.1
```

Reiniciar o PacketFence e o usuário deve estar bom para continuar.

Interface em cada VLAN

Porque o tráfego do DHCP é tráfego de difusão, uma alternativa para redes pequenas, com poucas VLANs local, é colocar uma interface de VLAN para cada VLAN no servidor PacketFence e ter uma `pfdhcplistener` interface de VLAN que escute.

No lado da rede, o usuário precisa ter certeza de que a VLAN realmente alcança todo o caminho de seu cliente para sua infraestrutura DHCP para o servidor PacketFence.

No lado PacketFence, primeiro o usuário precisa de um sistema operacional de interface VLAN, como abaixo. Armazenadas em `/etc/sysconfig/network-scripts/ifcfg-eth0.1010`:

```
# Engenharia VLAN
DEVICE=eth0.1010
ONBOOT=yes
BOOTPROTO=static
IPADDR=10.0.101.4
NETMASK=255.255.255.0
VLAN=yes
```

Então o usuário precisa especificar em `pf.conf` que o usuário está interessado nessa VLAN, declarando o tipo para `dhcp-listener`.

```
[interface eth0.1010]
mask=255.255.255.0
type=dhcp-listener
gateway=10.0.101.1
ip=10.0.101.4
```

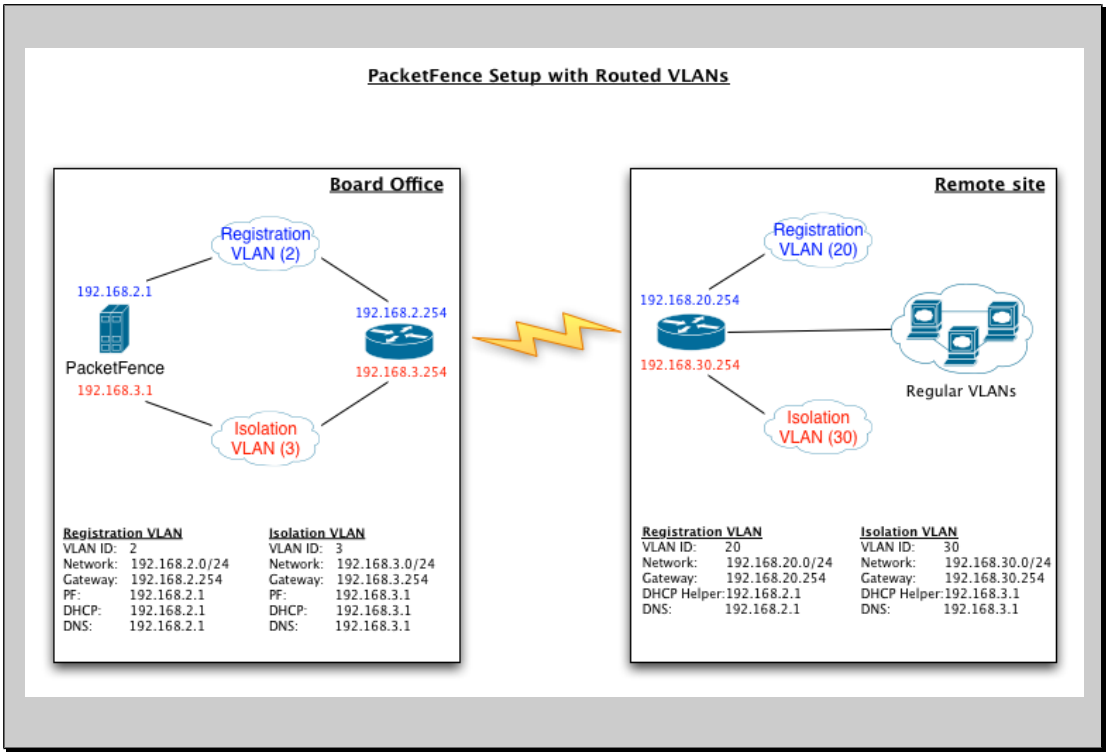
Repita o procedimento acima para toda a produção VLANs, em seguida reinicie o PacketFence.

Host de produção DHCP em PacketFence

É uma opção. Basta modificar `conf/dhcpd.conf` de modo que hospede a sua produção DHCP corretamente e certifique-se que um `pfdhcplistener` executa na mesma interface na qual a produção de DHCP é executada. Entretanto, note que isto **NÃO** é recomendado. Veja o lembrete para o porque.

Redes Roteadas

Se o seu isolamento e redes de registo não são localmente acessíveis (na camada 2) sobre a rede, mas roteada para o servidor PacketFence, o usuário terá de deixar o servidor PacketFence saber disso. PacketFence pode até mesmo fornecer DHCP e DNS nestas redes roteadas e fornecer uma configuração de interface fácil de usar.



Para dhcpd, certifique-se que os pedidos dos clientes DHCP estão corretamente encaminhados (Ajudantes IP nos roteadores remoto) para o servidor PacketFence. Certifique-se que o usuário seguiu as instruções no Servidor de Configuração DHCP e DNS (networks.conf) para sua rede localmente acessível.

Então o usuário precisa fornecer a informação encaminhada das redes para o PacketFence. O usuário pode fazê-lo através do GUI em Administration -> Networks (ou em `conf/networks.conf`).

Se considerarmos a arquitetura de rede ilustrado no esquema acima, `conf/networks.conf` será parecido com este:

```
[192.168.2.0]
netmask=255.255.255.0
gateway=192.168.2.1
next_hop=
domain-name=registration.example.com
```

```
dns=192.168.2.1
dhcp_start=192.168.2.10
dhcp_end=192.168.2.200
dhcp_default_lease_time=300
dhcp_max_lease_time=600
type=vlan-registration
named=enabled
dhcpd=enabled

[192.168.3.0]
netmask=255.255.255.0
gateway=192.168.3.1
next_hop=
domain-name=isolation.example.com
dns=192.168.3.1
dhcp_start=192.168.3.10
dhcp_end=192.168.3.200
dhcp_default_lease_time=300
dhcp_max_lease_time=600
type=vlan-isolation
named=enabled
dhcpd=enabled

[192.168.20.0]
netmask=255.255.255.0
gateway=192.168.20.254
next_hop=192.168.2.254
domain-name=registration.example.com
dns=192.168.2.1
dhcp_start=192.168.20.10
dhcp_end=192.168.20.200
dhcp_default_lease_time=300
dhcp_max_lease_time=600
type=vlan-registration
named=enabled
dhcpd=enabled

[192.168.30.0]
netmask=255.255.255.0
gateway=192.168.30.254
next_hop=192.168.3.254
domain-name=isolation.example.com
dns=192.168.3.1
dhcp_start=192.168.30.10
dhcp_end=192.168.30.200
dhcp_default_lease_time=300
dhcp_max_lease_time=600
type=vlan-isolation
named=enabled
```

```
dhcpd=enabled
```

Configuração do FreeRADIUS

Esta seção apresenta as etapas de configuração do FreeRADIUS. Em algumas ocasiões, um servidor RADIUS é obrigatória, a fim de dar acesso à rede. Por exemplo, o uso do WPA2-Enterprise (Wireless 802.1X), autenticação MAC e 802.1X com fios, todos requerem um servidor RADIUS para autenticar os usuários e os dispositivos, e então forçar a VLAN apropriada para o equipamento de rede. Nós recomendamos fortemente que o usuário instale o FreeRADIUS mesmo se o usuário não pretenda utilizar o recurso agora.

Instale os seguintes pacotes:

- packetfence-freeradius2

/etc/raddb/clients.conf

A partir do PacketFence 3.0, este passo é desnecessário. Como o usuário viu anteriormente neste guia, nós agora estamos usando o atributo `radiusSecret` no arquivo de configuração do switch.

Para versões anteriores ao PacketFence 3.0, o usuário ainda vai usar arquivo simples do cliente RADIUS. Substituir <...> com valores úteis a o usuário. O usuário precisa de uma entrada de cliente por dispositivo de rede.

```
client <useful_device_name> {
     ipaddr       = <network_device_ip_address>
     secret       = <radius secret>
}
```

/etc/raddb/packetfence.pm

Certifique-se de definir os parâmetros de configuração necessários em cima do arquivo. Defina a senha para a conta criada anteriormente sob a seção Interface de Administração baseada na Web.

```
# FreeRADIUS para comunicações com o PacketFence (configurações do
servidor SOAP)
WS_USER     => 'webservice',
WS_PASS     => 'password',
```

/etc/raddb/sql.conf

Certifique-se de definir as credencias adequadas para acessar o banco de dados do PacketFence.

```
    # Info de Conexão:
    server = "localhost"
    port = 3306
    login = "pf"
    password = "pf"
```

Opção 1: Autenticação no Active Directory (AD)

Substituir `/etc/raddb/modules/mschap` com a seguinte configuração:

```
mschap {
        use_mppe = yes
        require_encryption = yes
        require_strong = yes
        with_ntdomain_hack = yes
        ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{%
{Stripped-User-Name}:-%{mschap:User-Name:-None}} --challenge=%
{mschap:Challenge:-00} –nt-response=%{mschap:NT-Response:-00}"
}
```

Samba / Kerberos / Winbind

Instale SAMBA. O usuário pode usar as fontes ou usar o pacote para o seu OS. Para CentOS, o usuário pode usar:

```
wget ftp://ftp.sernet.de/pub/samba/3.5/centos/5/x86_64/samba3-3.5.6-
43.el5.x86_64.rpm
wget ftp://ftp.sernet.de/pub/samba/3.5/centos/5/x86_64/samba3-client-
3.5.6-43.el5.x86_64.rpm
wget ftp://ftp.sernet.de/pub/samba/3.5/centos/5/x86_64/samba3-utils-
3.5.6-43.el5.x86_64.rpm
wget ftp://ftp.sernet.de/pub/samba/3.5/centos/5/x86_64/samba3-winbind-
3.5.6-43.el5.x86_64.rpm
wget ftp://ftp.sernet.de/pub/samba/3.5/centos/5/x86_64/libwbclient0-
3.5.6-43.el5.x86_64.rpm

yum install ./samba*.rpm --nogpgcheck
```

Nota: Se o usuário tiver PCs Windows 7 na sua rede, o usuário precisa usar a versão 3.5.0 ou superior do SAMBA)

Quando feito com a instalação do samba, o usuário precisa modificar `/etc/krb5.conf`. Aqui está um exemplo para o domínio DOMAIN.NET:

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = DOMAIN.NET
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 DOMAIN.NET = {
  kdc = adserver.domain.net:88
  admin_server = adserver.domain.net:749
  default_domain = domain.net
 }
[domain_realm]
 .domain.net = DOMAIN.NET
 domain.net = DOMAIN.NET

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

Em seguida, editar /etc/samba/smb.conf. Novamente, aqui está um exemplo para nosso DOMAIN.NET

```
[global]
workgroup = DOMAIN
server string = pf_server_name
interfaces = 192.168.1.2/24
security = ADS
passdb backend = tdbsam
realm = DOMAIN.NET
encrypt passwords = yes
```

```
winbind use default domain = yes
client NTLMv2 auth = yes
preferred master = no
load printers = no
cups options = raw
idmap uid = 10000-45000
idmap gid = 10000-45000
log level = 1 winbind:5 auth:3
```

Depois disso, o usuário precisa iniciar o samba, e junta-se a máquina ao domínio

```
service smb start
chkconfig --level 345 smb on
net ads join -U administrator
```

Finalmente, inicie o winbind, e teste a configuração usando ntlm_auth

```
service winbind start
chkconfig --level 345 winbind on
chgrp radiusd /var/lib/samba/winbindd_privileged/
ntlm_auth –username myDomainUser
```

Opção 2: Autenticação Local

Adicionar entradas do seu usuário no final do arquivo `/etc/raddb/users` com o seguinte formato:

```
username    Cleartext-Password := "password"
```

Opção 3: Autenticação diante a OpenLDAP

```
Para ser contribuído...
```

Testes

Teste a sua configuração com radtest usando o seguinte comando e tenha certeza de obter uma resposta Access-Accept:

```
# radtest dd9999 Abcd1234 localhost 12 testing123
```

```
Sending Access-Request of id 74 to 127.0.0.1 port 1812
     User-Name = "dd9999"
     User-Password = "Abcd1234"
     NAS-IP-Address = 255.255.255.255
     NAS-Port = 12
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=74, length=20
```

Depurar

Primeiro, verifique o syslog, este é no qual os logs do módulo PacketFence estão. Mensagens syslog são armazenadas geralmente em `/var/log/messages`.

Se isso não ajudar, execute o FreeRADIUS no modo de depuração. Para fazê-lo, iniciá-lo usando o seguinte comando:

```
# radiusd -X
```

Iniciando os Serviços PacketFence

Uma vez que o PacketFence está totalmente instalado e configurado, inicie os serviços usando o seguinte comando:

```
service packetfence start
```

O usuário pode verificar usando o comando `chkconfig` que o serviço PacketFence é iniciado automaticamente no momento do boot.

Arquivos de Log

Aqui estão os arquivos de log mais importante do PacketFence:

- `/usr/local/pf/logs/packetfence.log` – Log do Núcleo PacketFence
- `/usr/local/pf/logs/access_log` – Apache – Log de acesso Captive
- `/usr/local/pf/logs/error_log` – Apache – Log de erro Captive Portal
- `/usr/local/pf/logs/admin_access_log` – Apache – Log de Acesso Web Admin/Serviços
- `/usr/local/pf/logs/admin_error_log` – Apache – Log de erro Web Admin/Serviços
- `/usr/local/pf/logs/admin_debug_log` – Apache – Log de Depuração Web

Administrativa

Existem outros arquivos de log em `/usr/local/pf/logs/` que poderiam ser relevantes dependendo do problema que está ocorrendo. Certifique-se de dar uma olhada neles.

O arquivo de configuração de log é `/usr/local/pf/conf/log.conf`. Ele contém a configuração para o arquivo `packetfence.log` (`Log::Log4Perl`) e o usuário normalmente não precisa modificá-lo.

Começando com 3.0, o usuário pode ver os arquivos de logs na Administração Web em Administration > Logs.

Configuração por exemplo

Aqui está um exemplo de configuração de ponta a ponta do PacketFence no modo "Hybrid" (modo VLAN e modo Inline ao mesmo tempo).

Suposições

Durante todo este exemplo de configuração, nós usamos as seguintes suposições para nossa infraestrutura de rede::

- Existem dois tipos diferentes de switches gerenciáveis em nossa rede: Cisco Catalyst 2900XL e Cisco Catalyst 2960, e um dispositivo não gerenciável.
- VLAN 1 é a VLAN "regular"
- VLAN 2 é a VLAN de registro (dispositivos não registrados serão colocados nessa VLAN)
- VLAN 3 é a VLAN de isolamento (dispositivos isolados serão colocados nessa VLAN)
- VLANs 2 e 3 são medidos em toda a rede
- VLAN 4 é a VLAN de detecção MAC (VLAN vazia)
- VLAN 4 deve ser definida em todos os switches que não suportam segurança por porta (em nosso exemplo, o Catalyst 2900XL não suporta segurança por porta com endereço MAC estático). Não há necessidade de colocá-lo na porta de tronco (trunk).
- VLAN 5 é a VLAN Inline (em Banda, para dispositivos não gerenciáveis)
- Queremos isolar os computadores usando Limewire (software peer-to-peer)
- Nós usamos o Snort como NIDS
- O tráfego monitorado pelo Snort é atravessado na eth1
- O servidor DHCP no PacketFence que vai cuidar da distribuição de endereços IP em VLANs 2, 3 e 5
- O servidor de DNS no PacketFence que vai cuidar de resolução de domínio em VLANs 2 e 3
- A configuração da rede fica assim:

VLAN ID	Nome VLAN	Sub-rede	Gateway	Endereço PacketFence

1	Normal	192.168.1.0/24	192.168.1.1	192.168.1.5
2	Registro	192.168.2.0/24	192.168.2.1	192.168.2.1
3	Isolation	192.168.3.0/24	192.168.3.1	192.168.3.1
4	Mac Detection			
5	Inline	192.168.5.0/24	192.168.5.1	192.168.5.1
100	Voice			

Interfaces de Rede

Aqui estão os scripts NICs de inicialização em PacketFence:

- `/etc/sysconfig/network-scripts/ifcfg-eth0`

```
DEVICE=eth0
BROADCAST=192.168.1.255
IPADDR=192.168.1.5
NETMASK=255.255.255.0
NETWORK=192.168.1.0
ONBOOT=yes
TYPE=Ethernet
```

- `/etc/sysconfig/network-scripts/ifcfg-eth0.2`

```
DEVICE=eth0.2
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.2.1
NETMASK=255.255.255.0
VLAN=yes
```

- `/etc/sysconfig/network-scripts/ifcfg-eth0.3`

```
DEVICE=eth0.3
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.3.1
NETMASK=255.255.255.0
VLAN=yes
```

- `/etc/sysconfig/network-scripts/ifcfg-eth0.5`

```
DEVICE=eth0.5
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.5.1
NETMASK=255.255.255.0
VLAN=yes
```

- `/etc/sysconfig/network-scripts/ifcfg-eth1`. Este NIC é usada para o espelho do tráfego monitorado pelo Snort.

```
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=none
```

Receptor de Trap

PacketFence usa snmptrapd como o receptor de trap. Ele armazena o nome da comunidade usada pelo switch para enviar traps no arquivo de configuração switch (`/usr/local/pf/conf/switches.conf`):

```
[default]
SNMPCommunityTrap = public
```

Configuração de Switch

Em nosso exemplo, vamos habilitar linkUp/linkDown em um 2900LX Cisco e Segurança por porta em um Cisco Catalyst 2960. Por favor, consulte o Guia de Configuração de Dispositivos de rede para a lista completa de switches suportados e instruções de configuração.

linkUp/linkDown + MAC Notification

global setup

```
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification
snmp-server host 192.168.1.5 trap version 2c public snmp mac-notification
```

```
mac-address-table notification interval 0
mac-address-table notification
mac-address-table aging-time 3600
```

Em cada interface

```
switchport mode access
switchport access vlan 4
snmp trap mac-notification added
```

Segurança por Porta

global setup

```
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.1.5 version 2c public port-security
```

Em cada interface, o usuário precisa inicializar a segurança por porta, autorizando um endereço MAC falso com os seguintes comandos

```
switchport access vlan 4
switchport port-security
switchport port-security maximum 2
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security mac-address 0200.0000.00xx
```

onde xx representa o índice da interface

Não se esqueça de atualizar o startup-config.

switches.conf

Veja Definição de Dispositivos de Rede para mais informações sobre o conteúdo desse arquivo.

Aqui estão os parâmetros (exceto os padrões) para o nosso exemplo

```
[default]
SNMPCommunityRead = public
SNMPCommunityWrite = private
SNMPommunityTrap = public
SNMPVersion = 1
vlans = 1,2,3,4,10
normalVlan = 1
```

```
registrationVlan = 2
isolationVlan = 3
macDetectionVlan = 4
VoIPEnabled = no

[192.168.1.100]
type = Cisco::Catalyst_2900XL
mode = production
uplink = 24

[192.168.1.101]
type = Cisco::Catalyst_2960
mode = production
uplink = 25
normalVlan = 10
radiusSecret=useStrongerSecret
```

Se você quer ter um nome de comunidade diferente para leitura/gravação para cada switch, declare-o em cada seção switch.

pf.conf

Aqui é o arquivo `/usr/local/pf/conf/pf.conf` para nossa configuração. Para mais informações sobre `pf.conf` veja a Configuração global no arquivo de seção (pf.conf).

```
[general]
domain=yourdomain.org
#Coloque seus servidores externos/Infra de DNS aqui
dnsservers=4.2.2.2,4.2.2.1
dhcpservers=192.168.2.1,192.168.3.1,192.168.5.1

[trapping]
registration=enabled
detection=enabled
range=192.168.2.0/24,192.168.3.0/24,192.168.5.0/24

[registration]
auth=ldap

[interface eth0]
mask=255.255.255.0
type=management
gateway=192.168.1.1
ip=192.168.1.5
```

```
[interface eth0.2]
mask=255.255.255.0
type=internal
enforcement=vlan
gateway=192.168.2.1
ip=192.168.2.1

[interface eth0.3]
mask=255.255.255.0
type=internal
enforcement=vlan
gateway=192.168.3.1
ip=192.168.3.1

[interface eth0.5]
mask=255.255.255.0
type=internal
enforcement=inline
gateway=192.168.5.1
ip=192.168.5.1

[interface eth1]
mask=255.255.255.0
type=monitor
gateway=192.168.1.5
ip=192.168.1.1
```

networks.conf

Aqui é o arquivo `/usr/local/pf/conf/networks.conf` para nossa configuração. Para mais informações sobre `networks.conf` veja Configuração DHCP e Servidor DNS.

```
[192.168.2.0]
netmask=255.255.255.0
gateway=192.168.2.1
next_hop=192.168.2.254
domain-name=registration.example.com
dns=192.168.2.1
dhcp_start=192.168.2.10
dhcp_end=192.168.2.200
dhcp_default_lease_time=300
dhcp_max_lease_time=600
type=vlan-registration
```



```
named=enabled
dhcpd=enabled

[192.168.3.0]
netmask=255.255.255.0
gateway=192.168.3.1
next_hop=192.168.3.254
domain-name=isolation.example.com
dns=192.168.3.1
dhcp_start=192.168.3.10
dhcp_end=192.168.3.200
dhcp_default_lease_time=300
dhcp_max_lease_time=600
type=vlan-isolation
named=enabled
dhcpd=enabled

[192.168.5.0]
netmask=255.255.255.0
gateway=192.168.5.1
next_hop=
domain-name=inline.example.com
dns=4.2.2.2,4.2.2.1
dhcp_start=192.168.5.10
dhcp_end=192.168.5.254
dhcp_default_lease_time=300
dhcp_max_lease_time=600
type=inline
named=disabled
dhcpd=enabled
```

Detalhes da aplicação Inline

Para ver outro parâmetro importante opcional que pode ser alterado para fazer a aplicação Inline, veja a seção Configuração da aplicação Inline.

A fim de ter o modo Inline funcionando corretamente, o usuário precisa habilitar o encaminhamento de ip em seus servidores. Para fazê-lo permanentemente, olhar no `/etc/sysctl.conf`, e definir a seguinte linha:

```
# Controla o encaminhamento de pacotes IP
net.ipv4.ip_forward = 1
```

Salve o arquivo, e emita um `sysctl -p` para atualizar a configuração do SO.

FreeRADIUS

/etc/raddb/clients.conf

A entrada cliente para o Cisco 2960.

```
client lab-cisco2960 {
     ipaddr       = 192.168.0.101
     secret       = useStrongerSecret
}
```

Componentes Opcionais

Bloqueando atividades maliciosas com violações

As violações de política permitem de o usuário restrinja o acesso de sistema do cliente baseado em violações de determinadas políticas. Por exemplo, se o usuário não permitir o tráfego do tipo P2P na sua rede, e o usuário estiver executando o software apropriado para detectá-lo e provocar uma violação de um determinado cliente, o PacketFence dará a esse cliente uma página "bloqueada" que pode ser personalizado para o seu desejo.

A fim de ser capaz de bloquear atividades maliciosas, o usuário precisa instalar e configurar o IDS SNORT para conversar com o PacketFence.

Snort

Instalação

O procedimento de instalação é bastante simples para o SNORT. Mantemos uma versão de trabalho no repositório do PacketFence. Para instalá-lo, basta executar o seguinte comando:

```
yum install snort
```

Configuração

O PacketFence fornece um modelo básico no qual o usuário precisa editar o arquivo snort.conf, dependendo da versão do Snort. O arquivo está localizado em `/usr/local/pf/conf`. Raramente é necessário alterar qualquer coisa nesse arquivo para fazer o Snort trabalhar e alertas de armadilha. Não edite o snort.conf localizado em `/usr/local/pf/var/conf`, todas as modificações serão destruídas em cada re-inicialização do PacketFence.

Violações

A fim de fazer o PacketFence reagir aos alertas do Snort, o usuário precisa explicitamente dizer o software para fazer isso. Caso contrário, os alertas serão descartados. Isso é muito simples de

realizar. Na verdade, o usuário precisa criar uma violação e adicionar o Snort alerta SID na seção de gatilho de uma violação.

Violações da política do PacketFence são controlados usando o arquivo de configuração `/usr/local/pf/conf/violations.conf`. O formato de violação é a seguinte:

```
[1234]
desc=Descrição de violação
priority=8
url=/content/index.php?template=<template>
redirect_url=/proxies/tools/stinger.exe
enable=Y
trigger=Detect::2200032,Scan::11808
actions=email,log,trap
vlan=isolationVlan
whitelisted_categories=
```

- `[1234]`: ID de violação. Qualquer inteiro, exceto 1200000-120099, o qual é exigido e reservado para as violações da administração.
- `desc`: Descrição da linha única de violação
- `priority`: Faixa de 1-10, com 1 a mais alta prioridade e 10 a mais baixa. Violações de maior prioridade serão endereçadas, primeiro, se um host tem mais de uma.
- `url`: A URL HTML do host será redirecionado ao mesmo tempo em violação. Este é geralmente uma URL local na forma `/content/index.php?template=...` onde `...` é o nome do modelo de correção para mostrar para o usuário. URLs completos, como http://myportal.com/violation1234/ também são suportados se `passthrough = proxy` é definido em `[trapping]`. Nesse caso, o Portal Captive vai fazer proxy reverso para a URL especificada. Deve ser tomado grande cuidado ao usar esse recurso, pois qualquer recurso fora do caminho especificado não irá carregar.
- `redirect_url`: O usuário é redirecionado para esta URL depois de reativado seu acesso à rede na página de re-mediação..
- `enable`: Se 'enable' está configurado para 'N', esta violação é desativada e violações adicionais deste tipo não serão adicionados.
- `trigger`: Método para fazer referência aos métodos de detecção externos, tais como, Detect (SNORT), Scan (Nessus), OS (DHCP detecção de impressões digitais), USERAGENT (assinatura do navegador), VENDORMAC (classe de endereço MAC), etc. Trigger é formatado com o seguinte tipo::ID. neste exemplo, 2000032 é a ID do snort e 11808 é o número de plugin Nessus. O ID Snort NÃO precisa ser igual ao ID de violação.
- `actions`: Esta é a lista de ações que será executada em uma adição de violação. As ações podem ser:
  - `log`: Uma mensagem de Log para o arquivo especificado em `[alerting].log`
  - `email`: E-mail o endereço especificado em `[alerting].emailaddr`, usando `[alerting].smtpserver`. Múltiplos emailaddr podem ser separados por vírgula.
  - `trap`: Isolar o host e colocá-lo em violação. Ele abre uma violação e deixa aberta.

Se a armadilha não está lá, uma violação é aberta e então fechada automaticamente

- `winpopup`: Enviar uma mensagem em janela popup. O usuário precisa configurar `[alerting].winserver`, `[alerting].netbiosname` em `pf.conf` quando se utiliza esta opção

- `external:` execute um comando externo, especificado em `[paths].externalapi`

❑ `vlan:` VLAN de destino no qual o PacketFence deve colocar o cliente quando uma violação desse tipo é aberta. O valor de VLAN pode ser:

- `isolationVlan`: Isolamento de VLAN como especificado em `switches.conf`. Este é o valor recomendado para a maioria dos tipos de violação.

- `registrationVlan`: Registro de VLAN como especificado em `switches.conf`.

- `normalVlan`: Normal VLAN como especificado em `switches.conf`. Nota: É preferível não prender e colocar em VLAN normal. Certifique-se de entender o que o usuário está fazendo.

❑ `whitelisted_categories:` Nós em uma categoria listada em `whitelisted_categories` não serão afetados por uma violação deste tipo. Formato é uma lista separada por vírgulas de nomes de categoria.

Também estão incluídos em `violation.conf`é a seção defaults. A seção defaults definirá um valor padrão para cada violação na configuração. Se um valor de configuração não é especificado no ID específico, o padrão será usado:

```
[defaults]
priority=4
max_enable=3
actions=email,log
auto_enable=Y
enable=N
grace=120
button_text=Enable Network
snort_rules=local.rules,bleeding-attack_response.rules,bleeding-
exploit.rules,bleeding-p2p.rules,bleeding-scan.rules,bleeding-virus.rules
vlan=isolationVlan
whitelisted_categories=
```

❑ `max_enable`: Número de vezes que um host será capaz de tentar remediar antes deles serem bloqueados e ter que chamar o help desk. Isso é útil para usuários que apenas "clicam" em páginas de violação.

❑ `auto_enable`: Especifica se um host pode se auto corrigir uma violação (ativar o botão de rede) ou se eles não podem nem devem ligar para o help desk.

- `grace`: Número de minutos antes da violação poder reaparecer. Isso é útil para permitir os hosts um tempo (no exemplo, 2 minutos) para fazer o download de ferramentas para corrigir a sua emissão, ou desligamento de sua aplicação peer-to-peer.
- `button_text`: Texto apresentado no formulário violação aos hosts.
- `snort_rules`: O arquivo de regras do Snort é responsabilidade dos administradores. Por favor, altere isso para apontar para seu arquivo(s) de regras de violação. Se você não especificar um caminho completo, o padrão é `/usr/local/pf/conf/snort`. Se o usuário precisa incluir mais de um arquivo, basta separar cada nome com uma vírgula.

`violations.conf` é carregado na inicialização.

Exemplo de Violação

No nosso exemplo, queremos isolar as pessoas usando o Limewire. Aqui, assumimos que o Snort está instalado e configurado para enviar alertas para o PacketFence. Agora precisamos configurar o isolamento no PacketFence.

Habilitar violação Limewire em `/usr/local/pf/conf/violations.conf` e configurá-la para executar um script externo

```
[2001808]
desc=P2P (Limewire)
priority=8
url=/content/index.php?template=p2p
actions=log,trap
enable=Y
max_enable=1
trigger=Detect::2001808
```

Submissão de Varredura (Nessus)

Instalação

Por favor, visite http://www.nessus.org/download/ para baixar e instalar o pacote Nessus para o seu sistema operacional. O usuário também vai precisar se registrar para o HomeFeed (ou o ProfessionalFeed) a fim de obter os plugins.

Depois de instalado o Nessus, siga a documentação do Nessus para a configuração do servidor Nessus, e criar um usuário para o PacketFence.

Configuração

Para que uma dada varredura do Nessus gere uma violação dentro do PacketFence, o usuário tem de configurar duas seções:

- `pf.conf`
  Aduste as configurações na seção `scan` como o seguinte:

```
[scan]
ssl=enabled
pass=userPassword
user=nessusUsername
port=1241
host=127.0.0.1
registration=enabled
nessusclient_file=basic-policy.nessus
nessusclient_policy=basic-policy
```

- `violations.conf`
  O usuário precisa criar uma seção nova da violação e tem que especificar

```
trigger=Scan::<violationId>
```

Na qual `violationId` é a ID do plugin Nessus para verificar. Depois de ter terminado a configuração, o usuário precisará recarregar o conteúdo da violação relacionada no banco de dados usando:

```
pfcmd reload violations
```

NOTA: Violações serão disparadas se o plugin Nessus é mais alta que uma vulnerabilidade de baixa severidade

Integração NessusClient

Novo desde a 1.8.3 é a capacidade de usar diretamente a linha de comando do cliente do nessus e arquivos .nessus. O formato do arquivo NessusClient está documentado em http://www.nessus.org/documentation/dot_nessus_file_format.pdf e podem ser facilmente gerados usando o cliente Nessus oficial.

O usuário terá de salvar seu arquivo .nessus no diretório `/usr/local/pf/conf/nessus/` e especificar seu nome de arquivo usando a definição de configuração `scan.nessusclient_file` . O usuário também tem de especificar o nome da diretiva usando a definição `scan.nessusclient_policy` . Depois disso, você pode executar sua varredura usando

```
pfcmd schedule now <IP>
```

NOTA: Se o usuário fornecer credenciais no arquivo .nessus, o usuário precisa habilitar a opção “Store passwords as plain text” no seu cliente Nessus.

Varredura em registro

Para executar uma verificação do sistema antes de dar acesso a um host na rede você precisa habilitar os parâmetros `scan.registration` em `pf.conf`.

Também é recomendado ajustar `scan.duration` para refletir o tempo gasto na verificação. Uma barra de progresso com esta duração será mostrado para o usuário enquanto ele está esperando. Por padrão, vamos definir esta variável para 60s.

Oinkmaster

Oinkmaster é um script perl que permite a possibilidade de atualizar as diferentes regras snort com muita facilidade. É simples de usar e instalar. Esta seção irá mostrar-lhe como implementar Oinkmaster para trabalhar com PacketFence e Snort.

Por favor, visite http://oinkmaster.sourceforge.net/download.shtml fazer o download oinkmaster. Um exemplo de arquivo de configuração do oinkmaster é fornecido em `/usr/local/pf/addons/snort/oinkmaster.conf`

Configuração

Aqui estão os passos para fazer o trabalho de Oinkmaster. Vamos supor que o usuário já baixou o arquivo mais recente oinkmaster:

- Descompacte o Oinkmaster recém-transferido
- Copie os scripts perl requerido em /usr/local/pf/oinkmaster. Você precisa copiar contrib e oinkmaster.pl
- Copie o oinkmaster.conf fornecido pelo PacketFence (veja a seção acima) em /usr/local/pf/conf
- Modificar a configuração para atender as suas próprias necessidades. Atualmente, o arquivo de configuração está definido para buscar o sangramento das regras.

Atualização de Regras

A fim de obter atualizações periódicas para as regras Snort para o PacketFence, nós simplesmente precisamos criar uma entrada no crontab com as informações corretas. O exemplo a seguir demonstra uma entrada no crontab para buscar as atualizações diariamente às 23:00 PM:

```
0 23 * * * (cd /usr/local/pf; perl oinkmaster/oinkmaster.pl -C conf/oinkmaster.conf -o conf/snort/)
```

Dispositivos de Rede Flutuante

A partir da versão 1.9, o PacketFence agora suporta dispositivos de rede flutuante. Um dispositivo de rede flutuante é um dispositivo para o qual o PacketFence tem um comportamento diferente em relação a um dispositivo regular. Esta funcionalidade foi originalmente adicionado para apoiar Pontos de Acesso móvel.

Agora o PacketFence só suporta dispositivos de rede flutuantes em switches Cisco configurado com porta de segurança.

Para um dispositivo regular, o PacketFence coloca na Vlan correspondente a seu status (Registro, Quarentena ou Vlan Regular) e autoriza-o na porta (port-security).

Um dispositivo de rede flutuante é um dispositivo que o PacketFence não gerencia como um dispositivo regular.

Quando um dispositivo de rede flutuante está ligado, o PacketFence deve deixar/permitir que todos os endereços MAC que serão conectados a esse dispositivo (ou aparecer na porta) e, se necessário, configure a porta como multi-vlan (trunk) e definir PVID e marcar VLANs na porta.

Quando um dispositivo de rede flutuante é desconectado, o PacketFence deve re-configurar a porta, como antes de ter sido ligado.

Aqui está como funciona:

- dispositivos de rede flutuante devem ser identificadas usando o endereço MAC.
- linkup/linkDown armadilhas não estão habilitados nos switches, somente a porta de segurança de armadilhas são.

  Quando o PacketFence recebe uma trap na porta de segurança para um dispositivo de rede flutuante, ele muda a configuração da porta de modo que:

- ele desabilita a segurança da porta
- ele define o PVID
- eventualmente define a porta como multi-vlan (trunk) e define o rotulo das Vlans
- permite armadilhas linkDown

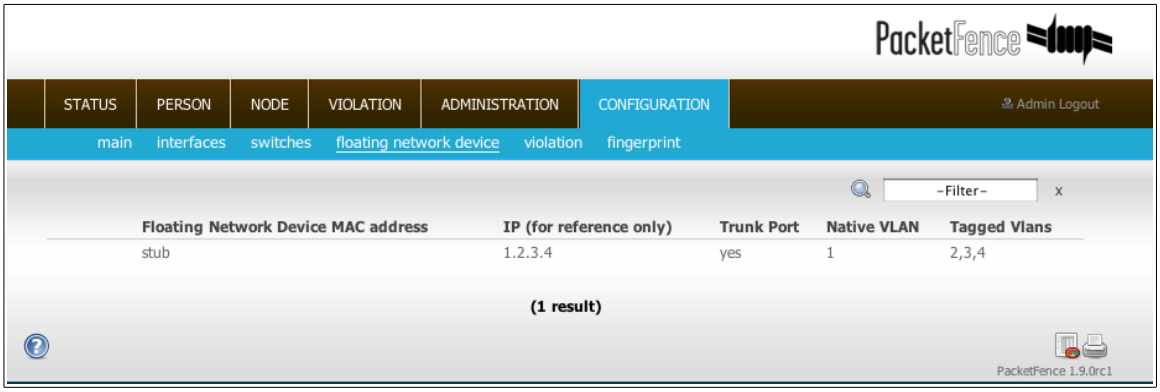
Quando o PF recebe uma armadilha linkDown em uma porta no qual um dispositivo de rede flutuante foi ligado, ele muda a configuração da porta de modo que:

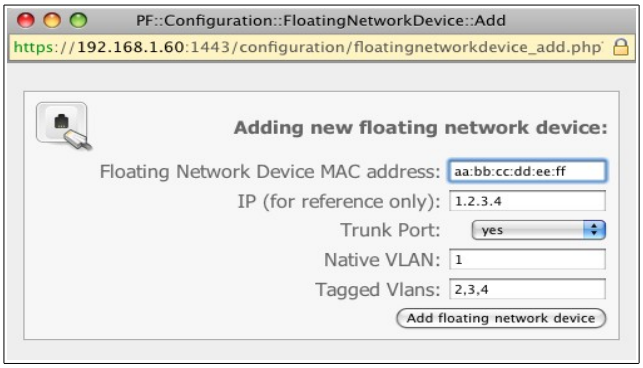
- ele permite a segurança da porta
- ele desabilita armadilhas linkDown

Identificação

Como mencionamos anteriormente, cada dispositivo de rede flutuante tem que ser identificado. Há duas maneiras de fazê-lo:

- editando `conf/floating_network_device.conf`
- através do GUI da Web, na guia Configuration -> Floating Network Device.





Aqui estão as configurações que estão disponíveis:

- Endereço MAC
- Endereço IP (no caso de um IP estático)
- trunkPort: yes/no. A porta deveria ser configurada como uma porta de muti-vlan?
- pvid: Vlan em que o PacketFence deve colocar a porta
- taggedVlan: lista separada por vírgula de VLANs. Se a porta é uma multi-vlan, estas são as Vlans que têm que ser marcados na porta.

Gerência de Convidado

PacketFence suporta a habilidade de gerenciar convidados, estabelecendo datas à expirar e atribuindo uma categoria diferente, que permitirá um acesso diferente para os recursos da rede.

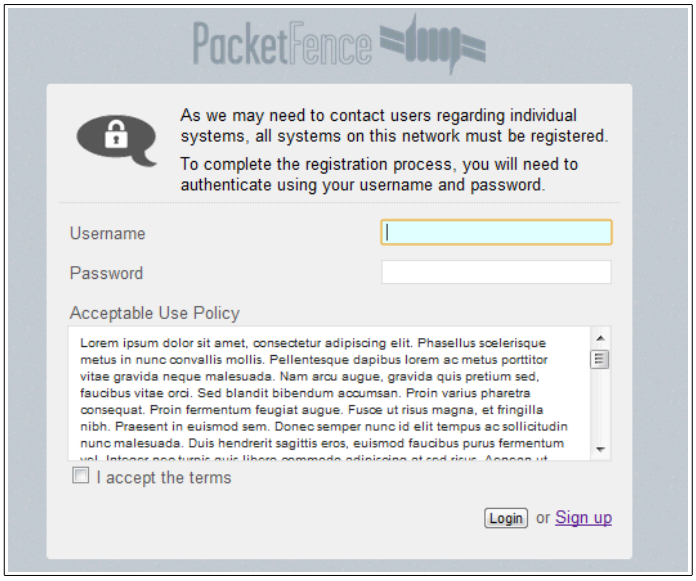
Os convidados podem se auto-registrar utilizando um código de ativação enviado para o seu telefone móvel ou eles podem usar seu endereço de e-mail e receber o link de ativação para ativar seu acesso à rede.

Convidados também podem ser criados usando uma interface web separada. Essa interface permitirá que os administradores do PacketFence ou gerentes de convidados, criar contas individuais, várias contas usando o prefixo (por exemplo: guest1, guest2, guest3...) ou importar datos de um arquivo CSV para criar contas. Uma duração de acesso e uma data de chegada também são personalizáveis.

Utilização

Auto-registro de Convidado

Auto-registro é habilitado por padrão. Faz parte do portal captive e pode ser acessado na página de registro clicando no link 'Sign up'.



Pré-registro de Convidado

Parte da interface de administração web, a interface de gerenciamento de convidados é ativada por padrão. É acessível através de uma interface própria, que pode usar um arquivo de usuários diferente para direitos de acesso.

```
https://ADMIN_IP:1443/guests/manage
```

Configuração

Auto-registro de Convidado

É possível modificar os valores do recurso padrão de auto-registro de convidado editando /usr/local/pf/conf/pf.conf.

Valores padrão estão localizados em /usr/local/pf/conf/pf.conf.defaults e documentação para todos os ajustes está disponível em /usr/local/pf/conf/documentations.conf.

```
[guests_self_registration]
modes=sms,email
category=guest
access_duration=7d
email_activation_timeout=10m
allow_localdomain=enabled
```

Para desativar o recurso de auto-registro, modificar a seguinte linha em /usr/local/pf/conf/pf.conf.

```
[guests_self_registration]
modes=
```

Note que o usuário precisará de um MTA válido configurado no PacketFence, para retransmitir corretamente e-mails relacionado ao módulo convidado. Se o usuário usar 'localhost' como smtpserver, o usuário precisa ter certeza de que um MTA está instalado e configurado no servidor.

Convidados auto-registrados são adicionados na aba persons da interface de administração web do PacketFence.

Pré-registro de Convidado

É possível modificar os valores do recurso padrão de pré-registro de convidado editando /usr/local/pf/conf/pf.conf.

Valores padrão estão localizados em /usr/local/pf/conf/pf.conf.defaults e documentação para todos os ajustes está disponível em /usr/local/pf/conf/documentations.conf.

```
[guests_pre_registration]
access_duration_choices=1h,3h,12h,1d,2d,3d,5d
default_access_duration=12h
category=guest
```

Para ativar o pré-registro de convidado para login através do portal captive, modifique a seguinte linha em /usr/local/pf/conf/pf.conf.

```
[registration]
auth=preregistered_guests
```

Administradores do PacketFence automaticamente tem acesso à interface de gerência de convidado. Também é possível criar usuários que somente terá acesso a esta interface em separado:

```
htpasswd /usr/local/pf/conf/guest-managers.conf <new_username>
```

O usuário recém-criado será capaz de acessar a interface imediatamente.

Note que o usuário precisará de um MTA válido configurado no PacketFence, para retransmitir corretamente e-mails relacionado ao módulo convidado. Se o usuário usar 'localhost' como smtpserver, o usuário precisa ter certeza de que um MTA está instalado e configurado no servidor.

Pré-registro de convidados são adicionados na aba persons da interface de administração web do PacketFence.

Declaração de Saúde (SoH)

Declaração de Saúde (SoH) é um produto que foi desenvolvido pela Microsoft. No mundo Microsoft, este é chamado Network Access Protection ou NAP. Em versões a partir do Windows XP SP2 para Windows 7, há um serviço NAP instalados que podem retransmitir informações de saúde (status de atualização do Antivírus, status de atualização do Windows, etc) para um servidor RADIUS ou um servidor DHCP. A seção abaixo explica como fazer políticas SoH com PacketFence.

Pacotes

Adicionando as funcionalidades SoH requer configuração específica RADIUS. Garantir que o usuário tenha pelo menos a verão 3.1 do pacote packetfence-freeradius2.

Instalação

Por padrão, nós desligamos SoH. Para ativar o suporte, simplesmente descomente as seguintes linhas em /etc/raddb/eap.conf.

```
soh=yes
soh-virtual-server = “soh-server”
```

Reinicie o serviço RADIUS depois.

No lado do cliente, para ativar SoH para EAP, faça o seguinte (Windows 7, por exemplo):

```
sc config napagent start=auto
sc start napagent

# 802.1X com fio
sc config dot3svc start=auto depend=napagent
sc start dot3svc

netsh nap client show config

# obter o valor 'ID' para o "EAP Quarantine Enforcement Cliente"
netsh nap client set enforce id=$ID admin=enable
```

O último passo é selecionar a 'Enforce Network Access Protection' checkbox sob as configurações de perfil EAP. Esses passos podem ser facilmente configurados usando GPOs.

Configuração de política SoH

A fim de aplicar uma política SoH, precisamos criá-la primeiro. Isso é feito usando uma interface separada acessível no mesmo servidor virtual como a UI administrativa. Ir para :

```
https://ADMIN_IP:1443/soh
```

Exemplo de Política

Vamos examinar uma situação exemplo. Suponha que o usuário queira exibir uma página de re-mediação para os clientes que não tem um antivírus ativado.

As três etapas gerais são: criar uma classe de violação para a condição, então crie um filtro SoH para adicionar a violação quando o 'antivírus é desativado', e finalmente recarregar as violações.

Primeiro, crie a violação adequada, quer através da interface de administração do usuário ou editando o arquivo `conf/violations.conf` files :

```
[4000001]
desc=No anti-virus enabled
url=/remediation.php?template=noantivirus
actions=trap,email,log
enabled=Y
```

NB. O usuário também pode querer definir outros atributos, tais como, auto_enable, grace, etc.

Quando feito com a violação, visite `https://localhost:1443/soh` e (edite o filtro chamado 'Default', ou) use o botão 'Add a filter' para criar um filtro chamado 'antivirus'. Clique em 'antivirus' na lista de filtros, e selecione 'Trigger violation' na ação drop-down. Digite o vid da violação criado acima, na caixa de entrada que aparece.

Em seguida, clique em 'Add a condition', e selecione 'Anti-virus', 'is', e "disabled" nas caixas drop-down que aparecem. Clique no botão 'Save filters'. Finalmente, recarregue as violações ou reiniciando o PacketFence ou usando o comando `pfcmd reload violations`.

O último passo é criar um novo modelo de re-mediação chamado `noantivirus.php` no sistema de arquivos no diretório `html/captive-portal/violations`. Edite-o para incluir o texto que deseja exibir para os usuários.

Capítulo 8

Melhores Práticas do Sistema operacional

Iptables

IPTables é agora inteiramente gerenciado pelo PacketFence. Entretanto, se o usuário precisa executar algumas regras personalizadas, o usuário pode modificar `conf/iptables.conf` para suas próprias necessidades. Entretanto, o modelo padrão deve funcionar para a maioria dos usuários.

Rotações de Log

PacketFence pode gerar uma grande quantidade de entradas de log em ambientes enormes de produção. É por isso que recomendamos usar o logrotate ou o log4perl para girar periodicamente seus logs.

Logrotate

Esta é a maneira mais fácil de girar seus logs. Na verdade, um script logrotate de trabalho é fornecido com o pacote PacketFence. Este script está localizado em `/usr/local/pf/addons`, e é configurado para fazer uma rotação de log semanalmente. Basta adicioná-lo à sua cronjobs logrotate existente.

Log4perl

Desta forma, log4perl é um pouco mais complexa para se conseguir, mas ainda é bastante simples. Existem 3 pacotes que você precisa obter de RPMForge:

- perl-Log-Dispatcher
- perl-Log-Dispatcher-FileRotate
- perl-Date-Manip

Uma vez que o usuário baixou os pacotes, o usuário precisará modificar o arquivo de

configuração de log (conf/log.conf) algo com o exemplo a seguir. Note-se que log4perl é quase o mesmo que log4j, então o usuário deve ser capaz de encontrar um monte de documentação on-line.

```
log4perl.appender.LOGFILE=Log::Dispatch::FileRotate
log4perl.appender.LOGFILE.filename=/usr/local/pf/logs/packetfence.log
log4perl.appender.LOGFILE.mode=append
log4perl.appender.LOGFILE.autoflush=1
log4perl.appender.LOGFILE.size=51200000
log4perl.appender.LOGFILE.max=5
log4perl.appender.LOGFILE.layout=PatternLayout
log4perl.appender.LOGFILE.layout.ConversionPattern=%d{MMM dd HH:mm:ss}
%X{proc}(%X{tid}) %p: %m (%M)%n
```

Alta Disponibilidade

Uma configuração de alta disponibilidade (ativo/passivo) para o PacketFence pode ser criada usando dois servidores PacketFence e os seguintes utilitários de código aberto:

- Linux-HA (www.linux-ha.org): Um daemon que fornece infraestrutura de cluster para seus clientes. Heartbeat seria o responsável por iniciar os serviços do PacketFence, eventualmente
- DRBD (www.drbd.org): Uma rede baseada em RAID-1.

Desde o PacketFence, a maioria armazena suas informações em um banco de dados MySQL. O PacketFence necessita de dois servidores redundantes para compartilhar esse banco de dados de um jeito ou de outro.

Existem diferentes opções para compartilhar o banco de dados entre os dois servidores PacketFence:

- Um servidor de banco de dados local MySQL em cada PacketFence configurado para armazenar suas bases de dados em uma partição remota (um LUN em um SAN, por exemplo)
  - O usuário tem de se certificar de que somente um servidor de banco de dados está em execução de cada vez (não duplo montar a partição)
- Um servidor de banco de dados local MySQL, em cada PacketFence, e replicação da partição de banco de dados usando DRBD
- Um servidor de banco de dados MYSQL remoto com a sua própria configuração de alta disponibilidade

Neste documento, descrevemos a segunda opção que envolve DRBD.

Nós assumimos que:

- o usuário está usando RedHat Enterprise 5 ou CentOS 5.
- pf1 é o primeiro servidor do PacketFence
- pf2 é o segundo servidor do PacketFence
- PacketFence está configurado corretamente em cada servidor
- ta partição DRBD é extensa 30G
- usamos HeartBeat v1

Criação da partição DRBD

Durante a instalação do sistema operacional, reduzir o tamanho da partição principal e criar uma nova (que será usado para o banco de dados MySQL replicado) de 30G. A fim de fazer isso, no VolGroup00:

- reduzir o tamanho da LogVol00 em 30G
- criar uma nova partição (ext3) chamado mysql: 30G. O usuário será solicitado para especificar onde esta nova partição será montada: entrar /data (ou qualquer outra coisa que é usado pelo Linux).
- após a re-inicialização do primeiro servidor, editar /etc/fstab e excluir a linha para /data.

Instalação do DRBD e Linux-HA

Use a seguinte linha para instalar os pacotes necessários:

```
yum install drbd83 kmod-drbd83 heartbeat heartbeat-pils heartbeat-stonith
```

Instalação e Configuração do DRBD

Inicializando e configurando o DRBD não é direto!

Recomendamos fortemente que o usuário leia a documentação on-line disponíveis no site do DRBD assim o usuário tem uma melhor idéia de como ele funciona ...

Aqui assumimos o nome da partição é mysql.

Carregar o módulo DRBD no kernel:

```
modprobe drbd
```

Editar /etc/drbd.conf e colocar o seguinte conteúdo:

```
global {
    usage-count yes;
}

common {
    protocol C;
}

resource mysql {
  syncer {
    rate 100M;
    al-extents 257;
  }

  startup {
    degr-wfc-timeout 120;    # 2 minutos.
  }

  disk {
    on-io-error   detach;
  }
  device        /dev/drbd0;
  disk          /dev/VolGroup00/mysql;
  meta-disk     internal;

  em pf1_server_name {
    address     x.x.x.x:7788;
  }

  em pf2_server_name {
    address     y.y.y.y:7788;
  }
}
```

sendo:

- *mysql* é o nome da partição que o usuário criou ao instalar o OS
- *pf1_server_name* e *pf2_server_name* pelos nomes de servidor real.
- *x.x.x.x* e *y.y.y.y* pelos endereços IP dedicados para o DRBD em cada servidor (use uma placa de rede dedicada para isso, não a principal com todos os IPs)

Tentar inicializar DRBD criando os metadados para a partição do mysql com o seguinte

comando:

```
drbdadm create-md mysql
```

O usuário poderá obter este tipo de mensagem:

```
md_offset 31474053120
al_offset 31474020352
bm_offset 31473057792

Encontrado sistema de arquivos ext3 que utiliza 30736384 kB
configuração atual deixa utilizável 30735408 kB

Tamanho do dispositivo seria truncado, o qual
iria corromper dados e resultar em
erros 'além do final de acesso do dispositivo'.
O usuário precisa
   * O uso de metadados externo (recomendado)
   * encolha este sistema de arquivos primeiro
   * Zerar o dispositivo (destruir o sistema de arquivos)
Operação recusada.

Comando 'drbdmeta 0 v08 /dev/VolGroup00/mysql internal create-md'
terminado com código de saída 40
drbdadm create-md mysql: saiu com o código 40
```

Se assim for, significa que o usuário precisa redimensionar a partição manualmente assim:

```
root@pf1 ~]# resize2fs -p -f /dev/VolGroup00/mysql 30735408K
resize2fs 1.39 (29-May-2006)
Redimensionar sistema de arquivos em /dev/VolGroup00/mysql para 7683852
(4k) blocks.
O sistema de arquivos em /dev/VolGroup00/mysql está agora com 7683852
blocos de comprimento.
```

Em seguida, inicializar a partição:

```
[root@pf1 ~]# drbdadm create-md mysql
md_offset 31474053120
al_offset 31474020352
bm_offset 31473057792

Encontrado sistema de arquivos ext3 que utiliza 30735408 kB
configuração atual deixa utilizável 30735408 kB
```

```
Mesmo que isso seria colocar o novo metadados em
espaço não utilizado, o usuário ainda precisa de confirmar, já que esta é
apenas uma suposição.

O usuário quer continuar?
[precisa digitar 'yes' para confirmar] yes

Gravando metadados...
registro de atividade de inicialização
Bitmap não inicializado
Novo bloco metadados drbd criado com sucesso.
```

Iniciar DRBD em ambos os servidores:

```
/etc/init.d/drbd start
```

Certifique-se de ver algo como isso em /proc/drbd:

```
...

 0: cs:Connected ro:Secondary/Secondary ds:Inconsistent/Inconsistent C
r----
    ns:0 nr:0 dw:0 dr:0 al:0 bm:0 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b
oos:30702640
```

Sincronizar os servidores, forçando um para se tornar o principal. Assim em pf1 faça:

```
drbdadm -- --overwrite-data-of-peer primary mysql
```

Depois de emitir este comando, a sincronização inicial completa será iniciada. O usuário será capaz de monitorar seu progresso através de /proc/drbd. Pode levar algum tempo dependendo do tamanho do dispositivo. Esperar até completar.

Certifique-se de DRBD é iniciado no tempo de boot:

```
chkconfig --level 2345 drbd on
```

Reinicie ambos os servidores.

Quando terminar, procure na /proc/drbd e certifique-se que o usuário veja:

```
...
```

```
 0: cs:Connected ro:Secondary/Secondary ds:UpToDate/UpToDate C r---
    ns:0 nr:0 dw:0 dr:0 al:0 bm:0 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b oos:0
```

Configuração do MySQL

Por padrão o MySQL coloca seus dados em /var/lib/mysql. A fim de replicar os dados entre os dois servidores, montamos a partição DRBD sob /var/lib/mysql.

Quando o primeiro MySQL iniciar, a partição deve ser montada.

A fim de fazê-lo:

No servidor master (o servidor que está a trabalhar), diga ao DRBD para se tornar o nó principal com:

```
drbdadm primary mysql
```

NOTA: mysql sendo o nome da partição DRBD.

Em /proc/drbd você deve ver algo como:

```
...
 0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate C r----
    ns:145068 nr:4448 dw:149516 dr:10490 al:31 bm:14 lo:0 pe:0 ua:0 ap:0
ep:1 wo:d oos:0
```

Monte a partição com:

```
mount /dev/drbd0 /var/lib/mysql
```

Iniciar o MySQL

```
service mysqld start
```

Execute o script de instalação segura, a fim de definir a senha de root, remover os bancos de dados de teste e usuário anônimo criado por padrão:

```
/usr/bin/mysql_secure_installation
```

Certifique-se que o MySQL não vai iniciar no momento da inicialização:

```
chkconfig --level 2345 mysqld off
```

Configuração do Heartbeat

Criar /etc/ha.d/ha.cf com o seguinte conteúdo:

```
bcast eth0
bcast eth1
keepalive 2
warntime 30
deadtime 60
auto_failback off
initdead 120
node pf1.example.org
node pf2.example.org
use_logd yes
```

Aqui assumimos que as conexões redundantes para o Heartbeat entre os dois servidores estão na eth0 e eth1

Criar /etc/ha.d/haresources com o seguinte conteúdo:

```
pf1.example.com Ipaddr2::x.x.x.x IfUp::eth0.y IfUp::eth0.z
drbddisk::mysql Filesystem::/dev/drbd0::/var/lib/mysql::ext3 mysqld
packetfence
```

- *x.x.x.x* é o endereço virtual do PF admin
- *eth0.y* é o nome do arquivo de configuração NIC (/etc/sysconfig/network-scripts/ifcfg_eth0.y) dedicado para o endereço IP em vlan y (registro, por exemplo).
- *eth0.z* é o nome do arquivo de configuração NIC (/etc/sysconfig/network-scripts/ifcfg_eth0.z) dedicado para o endereço IP em vlan z(isolamento, por exemplo).

Criar o /etc/ha.d/resource.d/ifup script que irá montar endereços IP em Registro, Isolamento, (eth0.y, etho0.z) com o seguinte conteúdo:

```
case "$2" in
        start)
                echo -n "Montando $1"
                /sbin/ifup $1
                echo "."
                ;;
        stop)
                echo -n "Desmontando $1"
                /sbin/ifdown $1
                echo "."
```

```
                ;;
        *)
                echo "Usage: $0 {start|stop}"
                exit 1
                ;;
esac
```

e torná-lo executável:

```
chmod 755 /etc/ha.d/resource.d/IfUp
```

Criar /etc/ha.d/authkeys com o seguinte conteúdo:

```
auth 1
1 sha1 10b245aa92161294df5126abc5b3b71d
```

e mudar os seus direitos como estão

```
chmod 600 /etc/ha.d/authkeys
```

Criar /etc/logd.cf com o seguinte conteúdo:

```
debugfile /var/log/ha-debug
logfile /var/log/ha-log
logfacility daemon
```

NOTA: Verifique se a porta 694 está aberta (através do iptables) em ambos os servidores

Iniciar o Heartbeat:

```
service heartbeat start
```

Olhe para o arquivo de log do Heartbeat /var/log/ha-log para certificar-se de que está tudo bem.

Habilitar o HB a iniciar automaticamente

```
chkconfig --level 345 heartbeat on
```

Configuração HA RADIUS

Se o usuário configurou o FreeRADIUS com a sua configuração sem fio e o usuário configurou a redundância, o usuário pode configurar o FreeRADIUS para responder a pedidos exclusivamente chegando ao IP virtual. A fim de fazê-lo, o usuário precisa modificar a configuração do RADIUS e adicione o RADIUS aos recursos gerenciados.

Configuração do RADIUS

Modificar as declarações listen no arquivo radiusd.conf pelo seguinte. Mudar o [VIP_IPV4_ADDRSS] com o seu endereço IP virtual:

```
listen {
     type = auth
     ipaddr = [VIP_IPV4_ADDRESS]
     port = 0
}
listen {
     ipaddr = [VIP_IPV4_ADDRESS]
     port = 0
     type = acct
}
```

Configuração do Heartbeat

Adicionar o RADIUS para os recursos gerenciados:

```
pf1.example.com Ipaddr2::x.x.x.x IfUp::eth0.y IfUp::eth0.z
drbddisk::mysql Filesystem::/dev/drbd0::/var/lib/mysql::ext3 mysqld
packetfence radiusd
```

Otimização de desempenho

Otimizações no MySQL

Ajustando o próprio MySQL

Se o usuário estiver o sistema PacketFence e está executando MUITO LENTO, isso poderia ser devido à sua configuração do MySQL. O usuário deve fazer o seguinte para ajustar o desempenho:

Verificar a carga do sistema

```
# uptime
11:36:37 up 235 days,  1:21,  1 user, load average: 1.25, 1.05, 0.79
```

Verifique iostat e CPU

```
# iostat 5
avg-cpu:  %user   %nice    %sys %iowait   %idle
           0.60    0.00    3.20   20.20   76.00
Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
cciss/c0d0       32.40         0.00      1560.00          0       7800
avg-cpu:  %user   %nice    %sys %iowait   %idle
           0.60    0.00    2.20    9.20   88.00
Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
cciss/c0d0        7.80         0.00        73.60          0        368
avg-cpu:  %user   %nice    %sys %iowait   %idle
           0.60    0.00    1.80   23.80   73.80
Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
cciss/c0d0       31.40         0.00      1427.20          0       7136
avg-cpu:  %user   %nice    %sys %iowait   %idle
           0.60    0.00    2.40   18.16   78.84
Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
cciss/c0d0       27.94         0.00      1173.65          0       5880
```

Como o usuário pode ver, a carga é 1.25 e o IOWait está atingindo um máximo de 20% - isso não é bom. Se sua espera IO é baixo, mas o seu MySQL está tomando mais de 50% de CPU

isso não é bom. Verifique seu instalador MySQL para as seguintes variáveis:

```
mysql> show variables;
| innodb_additional_mem_pool_size | 1048576
|
| innodb_autoextend_increment     | 8
|
| innodb_buffer_pool_awe_mem_mb   | 0
|
| innodb_buffer_pool_size         | 8388608
```

PacketFence depende muito do InnoDB, então o usuário deve aumentar o tamanho buffer_pool dos valores padrão.

Desligar PacketFence e MySQL

```
# /etc/init.d/packetfence stop
Desligando PacketFence ...
[...]
# /etc/init.d/mysql stop
Parando o MySQL:                                           [  OK  ]
```

Editar /etc/my.cnf (ou seu my.cnf local)

```
[mysqld]
# Coloque o buffer pool size para 50-80% da memória do seu computador
innodb_buffer_pool_size=800M
innodb_additional_mem_pool_size=20M
innodb_flush_log_at_trx_commit=2
# Permitir mais conexões
max_connections=700
# Coloque o tamanho do cache
key_buffer_size=900M
table_cache=300
query_cache_size=256M
# habilite log de consultas lentas
log_slow_queries = ON
```

Iniciar o MySQL e PacketFence

```
# /etc/init.d/mysqld start
Iniciando o MySQL:                                         [  OK  ]
# /etc/init.d/packetfence start
```

```
Iniciando o PacketFence...
[...]
```

Aguarde 10 minutos para o PacketFence mapear a rede inicial e verifique o iostat e CPU

```
# uptime
12:01:58 up 235 days,  1:46,  1 user, load average: 0.15, 0.39, 0.52
# iostat 5
Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
cciss/c0d0        8.00         0.00        75.20          0        376


avg-cpu:  %user   %nice    %sys %iowait   %idle
           0.60    0.00    2.99   13.37   83.03
Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
cciss/c0d0       14.97         0.00       432.73          0       2168
avg-cpu:  %user   %nice    %sys %iowait   %idle
           0.20    0.00    2.60    6.60   90.60
Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
cciss/c0d0        4.80         0.00        48.00          0        240
```

Ferramenta de otimização do MySQL

Recomendamos que o usuário execute a ferramenta MySQL Tuner em sua configuração de banco de dados após algumas semanas para ajudar o usuário identificar melhorias de configuração no MySQL.

http://blog.mysqltuner.com/download/

Mantendo tabelas pequenas

Com o tempo, algumas das tabelas crescerão e isso vai arrastar para baixo o desempenho (isto é especialmente verdadeiro em uma configuração sem fio).

Uma tal tabela é a tabela `locationlog`. Recomendamos que as entradas fechadas nesta tabela seja movida para a tabela de arquivo `locationlog_history` depois de algum tempo. Um registro fechado é aquele em que o campo `end_time` é definido como uma data (estritamente falando, é quando `end_time` não é nula e não é igual a 0).

Nós fornecemos um script chamado `database-backup-and-maintenance.sh` localizado em `addons/` que realiza essa limpeza, além de otimizar as tabelas no domingo e backups diários.

Evite problemas 'de conexões demais'

Em um contexto sem fio, tende a haver uma grande quantidade de conexões feitas ao banco de dados pelo nosso módulo freeradius. O valor padrão do MySQL tendem a ser baixas (100)

assim que nós encorajamos o usuário a aumentar esse valor para pelo menos 700. Ver http://dev.mysql.com/doc/refman/5.0/en/too-many-connections.html para mais detalhes.

Evite problemas 'Host <hostname> está bloqueado'

Em um contexto sem fio, tende a haver uma grande quantidade de conexões feitas ao banco de dados pelo nosso módulo freeradius. Quando o servidor é carregado, essas tentativas de conexão pode dar timeout. Se em tempos de conexão para fora durante a conexão, o MySQL irá considerar isso um erro de conexão e depois de 10 destes (por padrão) ele irá bloquear o host com um:

```
Host 'host_name' está bloqueado devido a muitos erros de conexão. Desbloqueie com 'mysqladmin flush-hosts'
```

Isso irá afiar o PacketFence para um desligamento, assim o usuário quer evitar isso a todo custo. Uma maneira de fazer isso é aumentar o número máximo de conexões (veja acima), para descarga periodicamente de hosts ou para permitir mais erros de conexão. Ver http://dev.mysql.com/doc/refman/5.0/en/blocked-host.html para mais detalhes.

Otimizações no Captive Portal

Evite a sobrecarga no portal captive, devido aos pedidos HTTP do não navegador

Por padrão, nós permitimos a cada consulta ser redirecionada e alcance o PacketFence para a operação de portal captive. Em muitos casos, isso significa que um monte de consultas iniciadas de não usuário chegarão ao PacketFence e desperdice seus recursos para nada, pois não são dos navegadores. (iTunes, Windows update, MSN Messenger, Google Desktop, ...).

Até agora, nós conhecemos a lista negra de clientes por comportar-se mal. Entretanto, uma abordagem completamente diferente pode ser tomada: lista branca somente de navegadores conhecidos.

Isto tem o efeito colateral desagradável de ser hostil com (bloqueio de) navegadores menos populares e dispositivos, assim este é desativado por padrão.

Se o usuário quiser ativar esse recurso, edite `conf/httpd.conf.d/block-unwanted.conf`, e descomente as seguintes linhas:

```
RewriteCond %{HTTP_USER_AGENT} !^Mozilla
RewriteCond %{HTTP_USER_AGENT} !^Opera
RewriteCond %{HTTP_USER_AGENT} !^BlackBerry
RewriteRule ^.*$ - [L,forbidden]
```

Isso permitirá os seguintes navegadores chegarem ao portal captive (mas nada mais):

- BlackBerry
- Firefox
- Google Chrome
- Internet Explorer
- Opera
- Safari

Capítulo 10

Perguntas Freqüentes

PacketFence FAQ está agora disponível online. Por favor, visite:
http://www.packetfence.org/support/faqs.html

Introdução técnica à aplicação de VLAN

Introdução

Atribuição de VLAN é atualmente realizada usando várias técnicas diferentes. Estas técnicas são compatível uma para outra, mas não na mesma porta do switch. Isto significa que o usuário pode usar as técnicas mais seguras e modernas para o seus mais recentes switches e outra técnica sobre as opções antigas que não suporta as mais recentes técnicas. Como o próprio nome indica, atribuição de VLAN significa que é o servidor PacketFence que atribui a VLAN para um dispositivo. Esta VLAN pode ser uma de suas VLANs ou pode ser uma VLAN especial na qual o PacketFence apresenta o portal captive para autenticação ou re-mediação.

Atribuição de VLAN efetivamente isola os seus hosts na camada 2 do modelo OSI que é o mais complicado método para contornar e é o que melhor se adapta ao seu ambiente, desde que 'cole' em sua metodologia atual de atribuição de VLAN.

Técnicas de Atribuição de VLAN

Segurança de Porta e SNMP

Baseia-se na segurança de porta, Traps SNMP. Um falso endereço MAC estático é atribuído a todas as portas, desta forma qualquer endereço MAC irá gerar uma violação de segurança e uma trap será enviada para o PacketFence. O sistema irá autorizar o MAC e definir a porta na VLAN correta. Suporte a VoIP é possível, mas complicado. Isso varia muito, dependendo do fornecedor do switch. Cisco é bem suportado, mas o isolamento de um PC por trás de um telefone IP leva a um dilema interessante: ou o usuário fecha a porta (e o telefone ao mesmo tempo) ou o usuário altera a VLAN de dados, mas o PC não faz DHCP (não detectaria se o link caiu) assim não pode chegar ao portal captive.

Além do dilema de isolamento VoIP, é a técnica que provou ser confiável e que tem o apoio da maioria dos fornecedores de switch.

Com Fio: 802.1X + Autenticação de MAC

802.1X fornece autenticação baseada em portas, que envolve a comunicação entre um suplicante, autenticador (conhecido como NAS), e o servidor de autenticação (conhecido como AAA). O suplicante (requerente) é frequentemente software em um dispositivo cliente, como um laptop, o autenticador é um switch Ethernet com fio ou ponto de acesso sem fio, e o servidor de autenticação é geralmente um servidor RADIUS.

O requerente (ou seja, dispositivo cliente) não é permitido o acesso através do autenticador para a rede até que a identidade do suplicante é autorizada. Com a autenticação baseada em portas 802.1X, o suplicante fornece credenciais, como nome de usuário / senha ou certificado digital, para o autenticador, e o autenticador encaminha as credenciais para o servidor de autenticação para verificação. Se as credenciais são válidas (na base de dados do servidor de autenticação), o requerente (dispositivo cliente) tem permissão para acessar a rede. O protocolo de autenticação é chamado Extensible Authentication Protocol (EAP), que tem muitas variantes. Ambos, suplicante e servidores de autenticação, precisam falar o mesmo protocolo EAP. Mais popular variante EAP é o PEAP-MSCHAPv2 (suportado pelo Windows / Mac OSX / Linux para autenticação no AD).

Neste contexto, PacketFence executa o servidor de autenticação (uma instância FreeRADIUS) e irá retornar a VLAN apropriada para o switch. Um módulo que integra em FreeRADIUS faz uma chamada remota ao servidor PacketFence para obter essa informação. Mais e mais dispositivos têm o suplicante 802.1X, o qual torna esta abordagem mais e mais popular.

Autenticação de MAC é um mecanismo novo introduzido por alguns fornecedores de switch para lidar com os casos em que um suplicante 802.1X não existe. Fornecedores diferentes têm nomes diferentes para ela. Cisco chama MAC Authentication Bypass (MAB), Juniper chama MAC RADIUS, a Extreme Networks chama Netlogin, etc. Após um período de tempo limite, o switch irá parar de tentar executar o 802.1X e irá retirar a autenticação MAC. Tem a vantagem de utilizar a mesma abordagem que 802.1X, exceto que o endereço MAC é enviado ao invés do nome de usuário e não há conversa de ponta a ponta EAP (sem autenticação forte). Usando a autenticação de MAC, dispositivos como impressora de rede ou telefones IP sem 802.1X IP podem ainda serem capazes de ter acesso à rede e a VLAN direto.

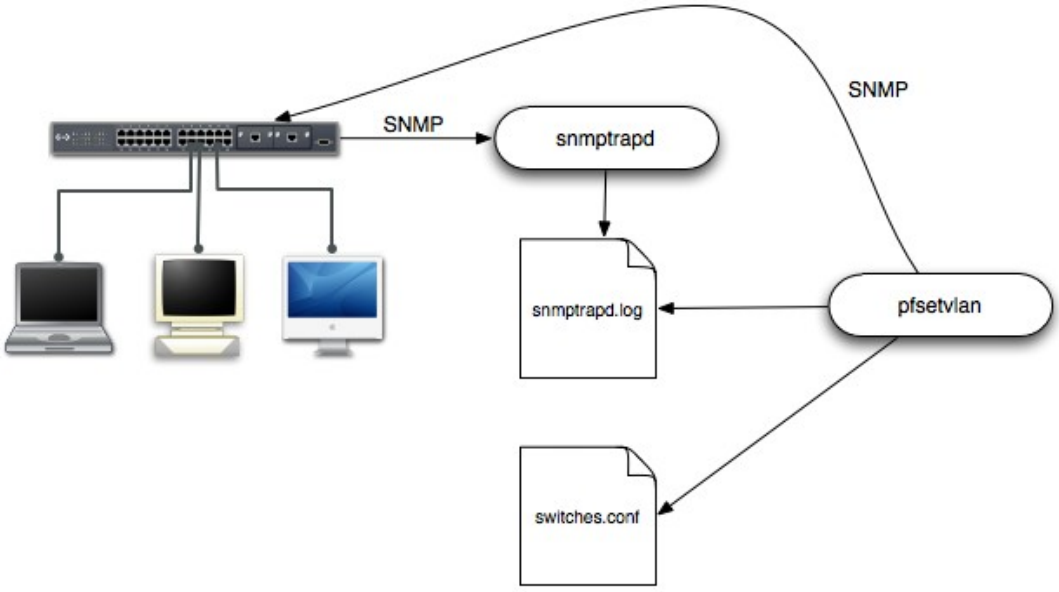
Sem-Fio: 802.1X + Autenticação de MAC

802.1X sem fio funciona como o com fio e autenticação de MAC é a mesma que autenticação de MAC com fio. Onde as coisas se alteram, é que o 802.1X é usado para configurar as chaves de segurança para a comunicação criptografada (WPA2-Enterprise), enquanto a autenticação de MAC é somente usada para autorizar, (permitir ou não) um MAC na rede sem fio.

Em redes sem fio, a configuração usual do PacketFence dita que o usuário configure dois SSIDs: um aberto e um seguro. O aberto é usado para ajudar os usuários a configurar o seguro corretamente e requer autenticação sobre o portal captive (que é executado em HTTPS).

Mais sobre SNMP traps e isolamento de VLAN

Quando o isolamento de VLAN está trabalhando através de traps SNMP todas as portas do switch (em que o isolamento de VLAN deve ser feito) deve ser configuradas para enviar traps SNMP para o host PacketFence. Em PacketFence, usamos snmptrapd como o receptor de trap SNMP. À medida que recebe os traps, que reformata-os e grava-os dentro de um arquivo simples: `/usr/local/pf/logs/snmptrapd.log`. O daemon concorrente pfsetvlan lê essas traps do arquivo simples e responde-lhes, definindo a porta do switch para a VLAN correta. Atualmente, suportamos switches desde Cisco, Edge-core, HP, Intel, Nortel e Linksys (adição de suporte para switches de outro fornecedor implica estender a classe pf::SNMP). Dependendo dos recursos de seus switches, pfsetvlan atuará em diferentes tipos de traps SNMP.



O usuário precisa criar uma VLAN de registro (com um servidor DHCP, mas não há encaminhamento para outras VLANs) em que o PacketFence irá colocar os dispositivos não registrados. Se você quer isolar os computadores que têm violações em aberto em uma VLAN separada, uma VLAN de isolamento também precisa ser criada.

linkUp/linkDown traps

Esta é a configuração mais básica e ela precisa de uma terceira VLAN: a VLAN de detecção de MAC. Não deve haver nada nesta VLAN (nenhum servidor DHCP) e não devem ser encaminhados para qualquer lugar, é apenas uma VLAN vazia.

Quando um host se conecta a uma porta do switch, o switch envia uma trap de linkUp para o PacketFence. Uma vez que leva algum tempo até que o switch aprenda o endereço MAC do

dispositivo recém-conectado, o PacketFence imediatamente coloca a porta na VLAN de detecção de MAC em que o dispositivo irá enviar pedidos de DHCP (sem resposta) para que o switch aprenda seu endereço MAC. Então pfsetvlan enviará periodicamente consultas SNMP para o switch até que o switch aprenda o MAC do dispositivo. Quando o endereço MAC é conhecido, pfsetvlan verifica seu status (existente? registrado? quaisquer violações?) no banco de dados e coloca a porta na VLAN apropriada. Quando um dispositivo é desconectado, o switch envia um trap 'linkDown' para o PacketFence que coloca a porta para a VLAN de detecção de MAC.

Quando um computador carrega, a inicialização da NIC gera várias alterações de estado de link. E todo momento o switch envia um trap linkUp e um linkDown para o PacketFence. Desde então, o PacketFence tem de agir em cada um desses traps, isso gera, infelizmente, algumas cargas desnecessárias sobre pfsetvlan. A fim de otimizar o tratamento de trap, o PacketFence pára cada segmento para uma trap "linkUp" quando recebe um trap " linkDown" na mesma porta. Mas, usando somente traps linkUp/linkDown não é a opção mais escalável. Por exemplo, em caso de falha de energia, se centenas de computadores iniciarem ao mesmo tempo, o PacketFence receberia uma grande quantidade de traps quase que instantaneamente e isso pode resultar na latência de conexão de rede ...

Traps de Notificação MAC

Se seus switches suportam traps de notificação MAC (MAC aprendeu, MAC removido), sugerimos que você ative-os, além dos traps linkUp/linkDown. Desta forma, pfsetvlan não precisa, depois de uma trap linkUp, consultar o switch continuamente até que o MAC seja finalmente aprendido. Quando ele recebe uma trap linkUp para uma porta na qual traps de notificação MAC também são ativados, ele só precisa colocar a porta na VLAN de detecção MAC e pode, então, desobstruir o segmento. Quando o switch aprende o endereço MAC do dispositivo, ele envia uma trap MAC aprendido (contendo o endereço MAC) para PacketFence.

Traps de Segurança por Porta

Na sua forma mais básica, o recurso de Segurança por Porta lembra características do endereço MAC conectado à porta do switch e permite apenas o endereço MAC que se comunique nessa porta. Se qualquer outro endereço MAC tentar se comunicar através da porta, a segurança por porta não vai permitir isso e enviará uma trap de segurança de porta.

Se o seus switches suportam esse recurso, recomendamos usá-lo ao invés de linkUp/linkDown e/ou notificações MAC. Por quê? Porque, enquanto um endereço MAC é autorizado em uma porta e é o único conectado, o switch não enviará trap se o dispositivo for reinicializado, plugado ou desplugado. Isso reduz drasticamente as interações entre os switches SNMP e PacketFence.

Quando o usuário ativar traps de segurança por porta o usuário não deve habilitar linkUp/linkDown nem traps de notificação MAC.

Capítulo 12

Introdução técnica à aplicação Inline

Introdução

Antes da verão 3.0 do PacketFence, não foi possível suportar dispositivos não gerenciáveis, tais como, switch de nível de entrada do consumidor ou pontos de acessos. Agora, com o novo modo Inline, o PacketFence pode ser usado em banda para esses dispositivos. Assim em outras palavras, o PacketFence se tornará o gateway dessa rede Inline, e o tráfego NAT usando IPTables para à Internet (ou para outra seção da rede). Vamos ver como ele funciona.

Configuração de dispositivo

Nenhum configuração especial é necessário no dispositivo não gerenciável. Essa é a beleza dele. O usuário só precisa garantir que o dispositivo está 'falando' sobre a VLAN Inline. Neste ponto, todo o tráfego será passado através do PacketFence, uma vez que é o gateway para esta VLAN.

Controle de Acesso

O controle de acesso depende inteiramente de IPTables. Quando um usuário não está registrado, e se conecta na VLAN Inline, o PacketFence lhe dará um endereço IP. Neste ponto, o usuário será marcado com não registrado no firewall, e todo o tráfego Web será redirecionado para o portal captive e outros bloqueados. O usuário terá de registrar através do portal captive como na aplicação de VLAN. Quando ele registra, o PacketFence muda a regra de firewall para permitir a marcação do endereço MAC do usuário atravesse-o.

Limitações

Aplicação Inline por causa de sua natureza tem diversas limitações que uma pessoa deve estar ciente.

- Todos atrás de uma interface Inline está na mesma camada 2 LAN
- Todos os pacotes de usuários autorizados passa pelo servidor PacketFence aumentando a

carga dos servidores consideravelmente: Planeje antecipadamente a capacidade

- ❑ Todos os pacotes de usuários autorizados passa pelo servidor PacketFence: é um ponto único de falha para acesso à Internet
- ❑ Não manipula redes roteadas

É por isso que é considerado como um homem pobre de fazer um controle de acesso. Temos evitado por um longo tempo por causa das limitações acima mencionadas. Dito isto, podendo executar tanto aplicação Inline e VLAN no mesmo servidor ao mesmo tempo é uma vantagem real: ele permite que os usuários mantenham o máximo de segurança, enquanto eles implementam hardware de rede novo e mais capaz, fornecendo um caminho de migração limpa para aplicação de VLAN.

Apêndice A: Ferramentas de Administração

pfcmd

pfcmd é a interface de linha de comando para a maioria das funcionalidades do PacketFence.

Quando executado sem argumentos pfcmd retorna uma mensagem de ajuda básica com todas as opções principais:

```
# /usr/local/pf/bin/pfcmd
Uso: pfcmd <command> [Opções]

class                   | ver violação de classes
config                  | consultar, definir, ou obter ajuda sobre
parâmetros de configuração pf.conf
configfiles             | empurre ou puxe arquivo de configuração dentro
de banco de dados
fingerprint             | ver DHCP Fingerprints
graph                   | gráficos de tendências
history                 | IP/MAC histórico
ifoctetshistorymac      | histórico contabilista
ifoctetshistoryswitch   | histórico contabilista
ifoctetshistoryuser     | histórico contabilista
interfaceconfig         | consultar/modificar os parâmetros de
configuração da interface
ipmachistory            | IP/MAC histórico
locationhistorymac      | histórico Switch/Port
locationhistoryswitch   | histórico Switch/Port
lookup                  | nó ou consulta contra armazenamento de dados
locais
manage                  | gerenciar entradas de nó
networkconfig           | consultar/modificar parâmetros de configuração
de rede
node                    | manipulação de nó
```

```
nodecategory            | manipulação de categoria do nó
person                  | manipulação de pessoa
reload                  | reconstruir tabelas de impressão digital ou
violações sem reiniciar
report                  | relatórios atuais de uso
schedule                | agendamento de scaneamento Nessus
service                 | start/stop/restart e obter status do daemon PF
switchconfig            | consultar/modificar os parâmetros de
configuração switches.conf
switchlocation          | ver a descrição e localização da porta no
switch
traplog                 | atualizar arquivos traplog RRD e gráficos ou
obter IPs do switch
trigger                 | ver e lançar triggers
ui                      | usado pela Interface web para criar hierarquias
de menu e painel
update                  | download canônico de impressão digital ou dados
OUI
version                 | pegue a versão instalada do PF e MD5s banco de
dados
violation               | manipulação de violação
violationconfig         | consultar/modificar parâmetros de configuração
violations.conf

Por favor, veja "pfcmd help <command>" para obter detalhes sobre cada
opção
```

A opção de visualização do nó mostra todas as informações contidas na tabela do nó banco de dados para um endereço MAC especificado

```
# /usr/local/pf/bin/pfcmd node view 52:54:00:12:35:02
mac|pid|detect_date|regdate|unregdate|lastskip|status|user_agent|
computername|notes|last_arp|last_dhcp|switch|port|vlan|dhcp_fingerprint
52:54:00:12:35:02|1|2008-10-23 17:32:16||||unreg||||2008-10-23
21:12:21|||||
```

pfcmd_vlan

pfcmd_vlan é a interface de linha de comando para a maioria das funcionalidades relacionados à VLAN de isolamento.

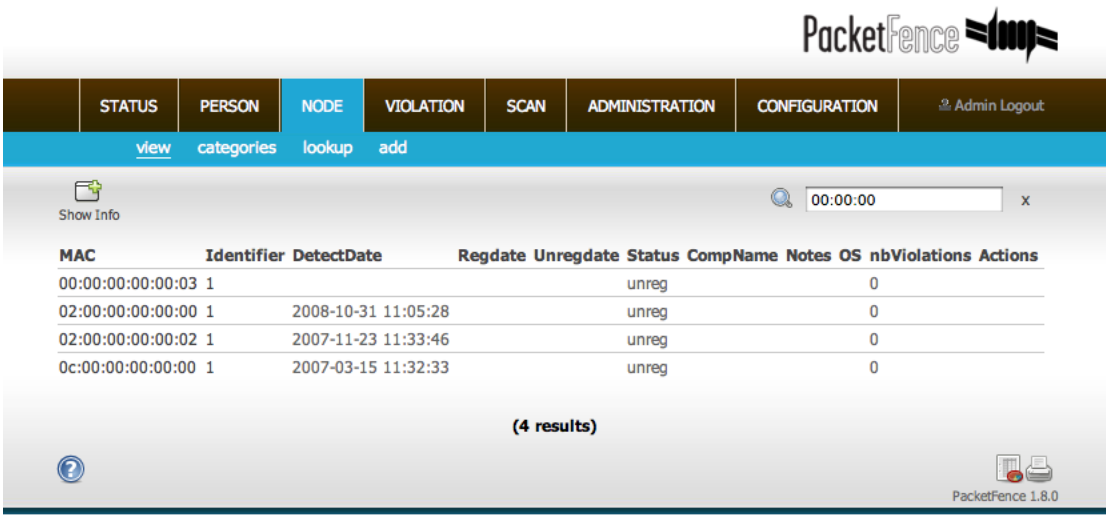
Mais uma vez, quando executado sem argumentos, uma tela de ajuda é apresentada.

```
# /usr/local/pf/bin/pfcmd_vlan
Uso:
    pfcmd_vlan command [opções]

Comando:
  -deauthenticate      de-autenticar um cliente dot1
  -getAlias            mostrar a descrição da porta do switch
especificada
  -getAllMACs          mostrar todos MAC's em todas as portas do switch
  -getHubs             mostrar portas do switch com vários MAC's
  -getIfOperStatus     mostrar o status operacional da porta especificada
no switch
  -getIfType           mostrar o ifType na porta especificada do switch
  -getLocation         mostrar em que porta do switch o MAC é encontrado
  -getMAC              mostrar todos os MAC's na porta do switch
especificado
  -getType             mostrar tipo de switch
  -getUpLinks          mostrar os upLinks do switch especificado
  -getVersion          mostrar versão do OS no switch
  -getVlan             mostrar a VLAN na porta especificada do switch
  -getVlanType         mostrar o tipo de porta especificada
  -help                breve mensagem de ajuda
  -isolate             definir a porta do switch para a VLAN de
isolamento
  -man                 documentação completa
  -reAssignVlan        rê-atribuir uma porta do switch a VLAN
  -resetVlanAllPort    redefinir VLAN em todas as portas sem UpLink no
switch especificado
  -resetVlanNetwork    redefinir VLAN em todas as portas sem UpLink de
todos os switches gerenciados
  -setAlias            definir a descrição da porta do switch
especificado
  -setDefaultVlan      definir a porta do switch para a VLAN padrão
  -setIfAdminStatus    definir o status de administrador da porta
especificada do switch
  -setVlan             definir VLAN na porta especificada do switch
  -setVlanAllPort      definir VLAN em todas as portas sem UpLink do
switch especificado

Opções:
  -alias               descrição da porta do switch
  -ifAdminStatus       ifAdminStatus
```

```
-ifIndex            porta do switch ifIndex
-mac                endereço MAC
-showMACVendor      mostrar o fornecedor MAC
-showPF             mostrar informações adicionais disponíveis no PF
-switch             descrição do switch
-verbose            nível de detalhamento de log
                      0: mensagens fatal
                      1 : mensagens de alerta
                      2 : mensagens de informação
                    > 2 : debug completo
-vlan               VLAN
```

Web Admin GUI

A Web Admin GUI, acessível usando https na porta 1443, mostra as mesmas informações disponíveis usando pfcmd.



Apêndice B : Manual de Configuração do FreeRADIUS 2

Uma vez que nós fornecemos um pacote RPM que contém pré-construídos arquivos de configuração RADIUS, esses arquivos não precisam mais serem modificados à mão. No entanto, considere esta seção como uma referência.

/etc/raddb/sites-enabled/default

Certifique-se o authorize{}, authenticate{} e post-auth{} seções como isto:

```
authorize {
     preprocess
     eap {
           ok = return
     }
     files
     expiration
     logintime
     perl
}

authenticate {
     Auth-Type MS-CHAP {
           mschap
     }
     eap
}

post-auth {
     perl
}
```

/etc/raddb/sites-enabled/inner-tunnel

Certifique-se o authorize{}, authenticate{} e post-auth{} seções como isto:

```
authorize {
```

```
     preprocess
     eap {
           ok = return
     }
     files
     expiration
     logintime
     perl
}

authenticate {
     Auth-Type MS-CHAP {
           mschap
     }
     eap
}

post-auth {
     perl
}
```

/etc/raddb/users

Adicione as seguintes linhas onde definimos que sem EAP-messages devem, por padrão, levar a uma aceitação de autenticação.

```
DEFAULT EAP-Message !* "", Auth-Type := Accept
```

Comentar ou apagar todas as outras declarações.

Opcional: Configuração com ou sem fio 802.1X

Gerar material criptográfico para o túnel EAP (802.1X) para o trabalho. Executar como root:

```
cd /etc/raddb/certs
make
```

/etc/raddb/eap.conf

Certifique-se este arquivo se parece com:

```
eap {
     default_eap_type = peap
```

```
	timer_expire     = 60
	ignore_unknown_eap_types = no
	cisco_accounting_username_bug = no
	max_sessions = 2048

	md5 {
	}
	tls {
		certdir = ${confdir}/certs
		cadir = ${confdir}/certs
		private_key_file = /usr/local/pf/conf/ssl/server.key
		certificate_file = /usr/local/pf/conf/ssl/server.crt
		dh_file = ${certdir}/dh
		random_file = ${certdir}/random
		cipher_list = "DEFAULT"
		make_cert_command = "${certdir}/bootstrap"
		cache {
			enable = no
			lifetime = 24 # hours
			max_entries = 255
		}
	}
	ttls {
		default_eap_type = md5
		copy_request_to_tunnel = yes
		use_tunneled_reply = yes
		virtual_server = "inner-tunnel"
	}
	peap {
		default_eap_type = mschapv2
		copy_request_to_tunnel = yes
		use_tunneled_reply = yes
		virtual_server = "inner-tunnel"
	}
	mschapv2 {
	}
}
```

Apêndice C: Configuração legada do FreeRADIUS 1.x

Desde o PacketFence 1.9.0 recomendamos o uso do FreeRADIUS 2.x sobre 1.x.

Esta documentação é disponibilizada aqui para o histórico de referência.

Configuração FreeRADIUS 1.x

Certifique-se de instalar os seguintes pacotes:

- freeradius

/etc/raddb/clients.conf

Adicione as seguintes linhas:

```
client 192.168.0.3 {
  secret = secretKey
  shortname = AP1242
}
```

/etc/raddb/radiusd.conf

Adicione as seguintes linhas à seção de módulos {}:

```
perl {
     module = ${confdir}/rlm_perl_packetfence.pl
}
```

Certifique-se a seção authorize{} é parecido com este:

```
authorize {
     preprocess
     eap
```

```
     files
     perl
}
```

Certifique-se a seção post-auth{} é parecido com este:

```
post-auth {
     perl
}
```

Certifique-se a seção mschap{} é parecido com este:

```
mschap {
     authtype = MS-CHAP
     use_mppe = yes
     require_encryption = yes
     require_strong = yes
     with_ntdomain_hack = yes
     ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%
{mschap:User-Name:-None} --challenge=%{mschap:Challenge:-00} --nt-
response=%{mschap:NT-Response:-00}"
}
```

/etc/raddb/eap.conf

Certifique-se este arquivo se parece com:

```
eap {
     default_eap_type = peap
     timer_expire     = 60
     ignore_unknown_eap_types = no
     cisco_accounting_username_bug = no

     md5 {
     }

     leap {
     }

     gtc {
```

```
            auth_type = PAP
    }

    tls {
            private_key_file = /usr/local/pf/conf/ssl/keyfile.key
            certificate_file = /usr/local/pf/conf/ssl/certfile.crt
            CA_file = /usr/local/pf/conf/ssl/CAfile.crt
            dh_file = /dev/null
            random_file = /dev/urandom
    }

    peap {
            default_eap_type = mschapv2
    }

    mschapv2 {
    }
}
```

/etc/raddb/users

Adicione as seguintes linhas onde definimos que sem EAP-messages devem, por padrão, levar a uma aceitação de autenticação.

```
DEFAULT EAP-Message !* "", Auth-Type := Accept
```

/etc/raddb/rlm_perl_packetfence.pl

Este script perl usa o atributo de pedido RADIUS Calling-Station-Id, contendo o MAC da estação sem fio, para determinar o registo e status de violação. Baseado nessas informações, ele define os atributos de reposta RADIUS Tunnel-Medium-Type, Tunnel-Type e Tunnel-Private-Group-ID. O AP, após a recepção desses três atributos, então confina a estação sem fio para a VLAN especificada.

Certifique-se de definir os parâmetros de configuração necessários em cima do arquivo. Principalmente, as tags VLAN usada em seu ambiente e as credenciais PacketFence do banco de dados.

```
# Configurações de conexão do banco de dados
DB_HOSTNAME => 'localhost',
DB_NAME     => 'pf',
DB_USER     => 'pf',
DB_PASS     => 'pf',
```

```
# Configuração VLAN
VLAN_GUEST        => 5,
VLAN_REGISTRATION => 2,
VLAN_ISOLATION    => 3,
VLAN_NORMAL       => 1
```

Testes

Teste a sua configuração com radtest usando o seguinte comando e tenha certeza de obter uma resposta Access-Accept:

```
# radtest dd9999 Abcd1234 localhost 12 testing123

Sending Access-Request of id 74 to 127.0.0.1 port 1812
     User-Name = "dd9999"
     User-Password = "Abcd1234"
     NAS-IP-Address = 255.255.255.255
     NAS-Port = 12
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=74, length=20
```

Depurar

A fim de iniciar o FreeRadius no modo de depuração, iniciá-lo usando o seguinte comando:

```
# radiusd -X
```

Capítulo 16

Informações Adicionais

Para mais informações, consulte os arquivos de correio ou envie suas perguntas para nós. Para mais detalhes, consulte:

packetfence-announce@lists.sourceforge.net: Anúncios Públicos (novos lançamentos, avisos de segurança etc.) sobre PacketFence

packetfence-devel@lists.sourceforge.net: Discussão de desenvolvimento PacketFence

packetfence-users@lists.sourceforge.net: O usuário e discussões de uso

Suporte Comercial e Informações de Contato

Para quaisquer perguntas ou comentários, não hesite em contactar-nos escrevendo um e-mail para:

support@inverse.ca

Inverse (http://inverse.ca) Oferece serviços profissionais ao redor do PacketFence para ajudar as organizações a implantar a solução, personalizar migrar versões ou de outro sistema, ajuste de desempenho ou alinhando com as melhores práticas.

Tarifas por hora ou pacotes de suporte são oferecidos para melhor atender às suas necessidades.

Por favor, visite http://inverse.ca/support.html para mais detalhes.

Capítulo 18

GNU Free Documentation License

Consulte http://www.gnu.org/licenses/fdl-1.2.txt para a licença completa.