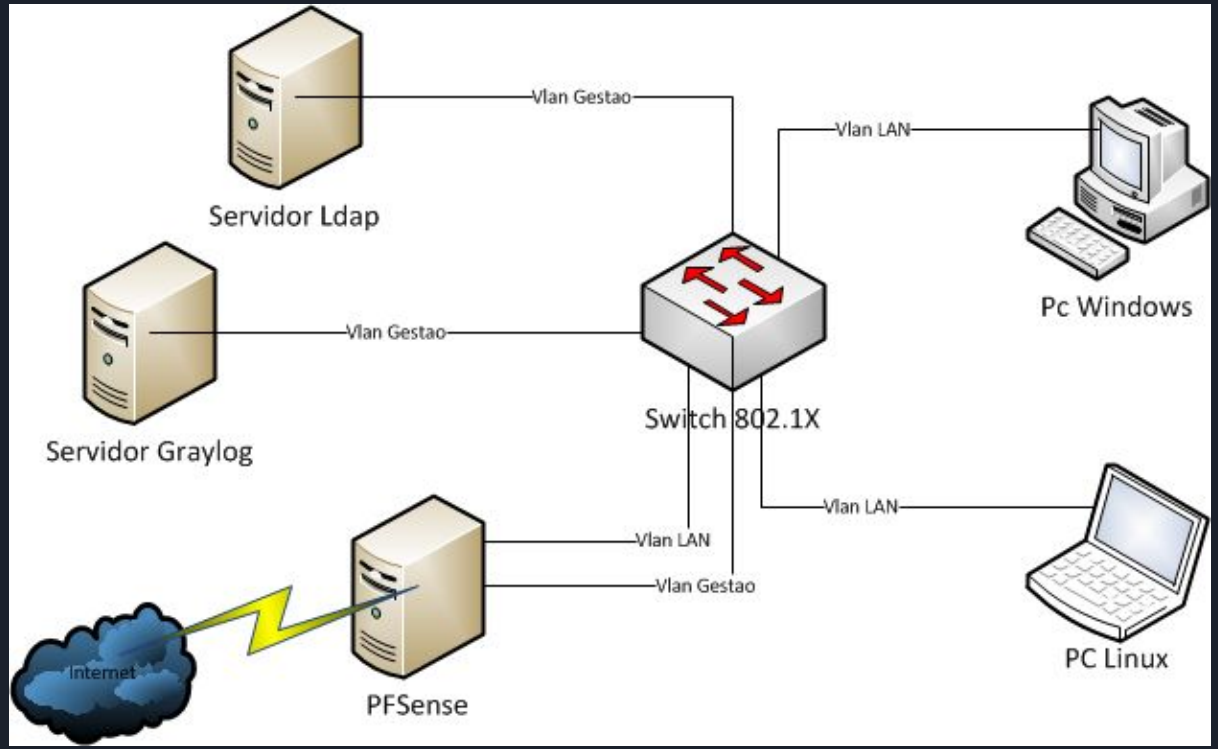
Rastreabilidade de utilizadores em redes privadas

Eduardo Costa & Tiago Pedrosa
raposo@ipb.pt | riftman@ipb.pt

ACK:
Rui Gonçalo - a35937@alunos.ipb.pt
Paulo Ferreira - a34960@alunos.ipb.pt

Como analisar um evento ou incidente quando a informação inicial se refere a um IP atrás de um NAT ?

O Cenário


Vlan Gestao
Servidor Ldap
Vlan LAN
Pc Windows
Vlan Gestao
Servidor Graylog
Switch 802.1X
Vlan LAN
Vlan LAN
Vlan Gestao
Internet
PFSense
PC Linux

Equipamento

Rede para testes

- Máquina para PFSense
- Máquina para Graylog
- Servidor LDAP
- Switch com suporte 802.1X
- Máquinas clientes com windows e linux

Procedimento Inicial

1. Configuração da Rede
2. Instalação e configuração do PFSense
3. Configuração 802.1X no switch e no PFSense o radius
4. Configuração do registo das conexões NAT estabelecidas
5. Instalação e configuração do Graylog
6. Configuração e testes de envio dos logs do PFSense para o Graylog
7. Teste autenticação, acesso e análise de logs

Rede

Foi utilizado um switch Hp procurve 2510G-24.

VLANs:

- Gestão.
- LAN.

802.1X:

- aaa authentication port-access eap-radius
- radius-server host IP key SHARED-KEY
- aaa port-access gvrp-vlans
- aaa port-access authenticator 13-14
- aaa port-access authenticator 16-20
- aaa port-access authenticator active

No PFsense configuraram-se os seguintes interfaces:

- WAN -> ale0 -> v4/DHCP4: 192.168.0.192/24
- LAN -> fxp0 -> v4: 192.168.1.1/24
- OPT1 -> fxp1 -> v4: 192.168.2.1/24

PFSense

- Após instalação base
- Gestor de pacotes -> Instalar freeRadius2
  - Configurar um novo cliente para o switch, IP, shortname e SHAREDSECRET
  - Associar ao interface OPT1
  - Ir às opções do LDAP e configurar para o radius fazer uso do servidor de LDAP existente na rede de gestão
- Verificar que as regras de firewalling deixam passar o tráfego no interface OPT1

Graylog

- Usamos uma base Ubuntu Server 16.06
- Instalamos:
  - openjdk-8-jre-headless uuid-runtime pwgen mongodb-server
  - elasticsearch - cluster.name: graylog
  - graylog-server
- Configurou-se a password para o graylog-server
- Ativaram-se a rest api e o frontend web

Graylog: Conf para recepcionar os logs do PF

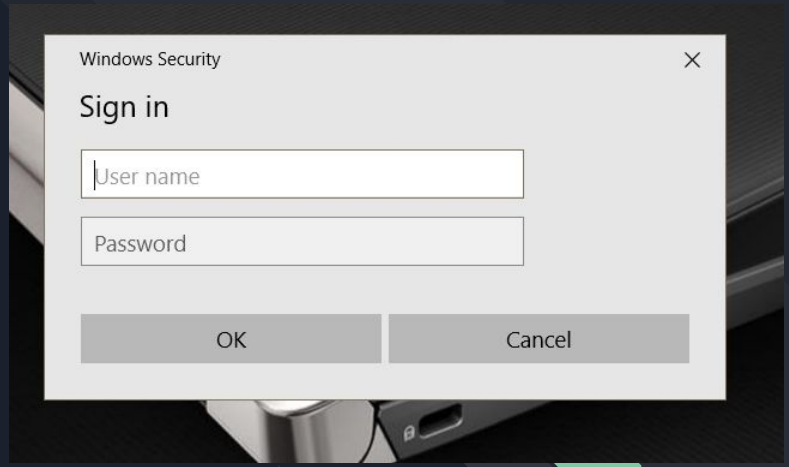
- Configurou-se o rsyslog para receber os logs e encaminhar para o graylog
  - Ativar os serviços módulos e input no rsyslog.conf
  - Criar template para o gray log (/etc/rsyslog.d/90-graylog.conf)
    - ```
      $template GRAYLOGRFC5424,"%protocol-version% %timestamp:::date-rfc3339% %HOSTNAME% %app-name% %procid% %msg%\n"
      *.* @127.0.0.1:5141;GRAYLOGRFC5424
      ```
  - Via interface web do graylog iniciar um novo input
    - System > Inputs > Select input > Syslog UDP > Launch new input
      - Title: pfsense
        Bind address: 127.0.0.1
        Port: 5141
  - Configuraram-se extratores para os logs do pfsense
  - DHCP: regex_value: .dhcpd\s-\s\sDHCPACK
  - Radius: regex_value: .radiusd\s[0-9]{1,45}\s\sLogin\sOK:\s([.?])
  - Radius mac: regex_value: .radiusd\s[0-9]{1,45}\s\sLogin\sOK:\s.(([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2}))
      ```

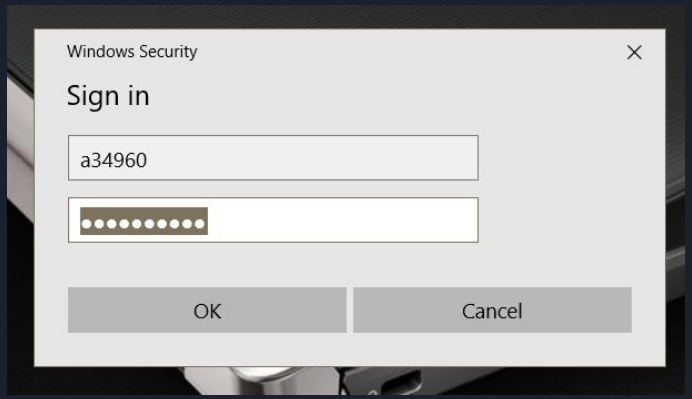
PFsense: Logs -> Graylog

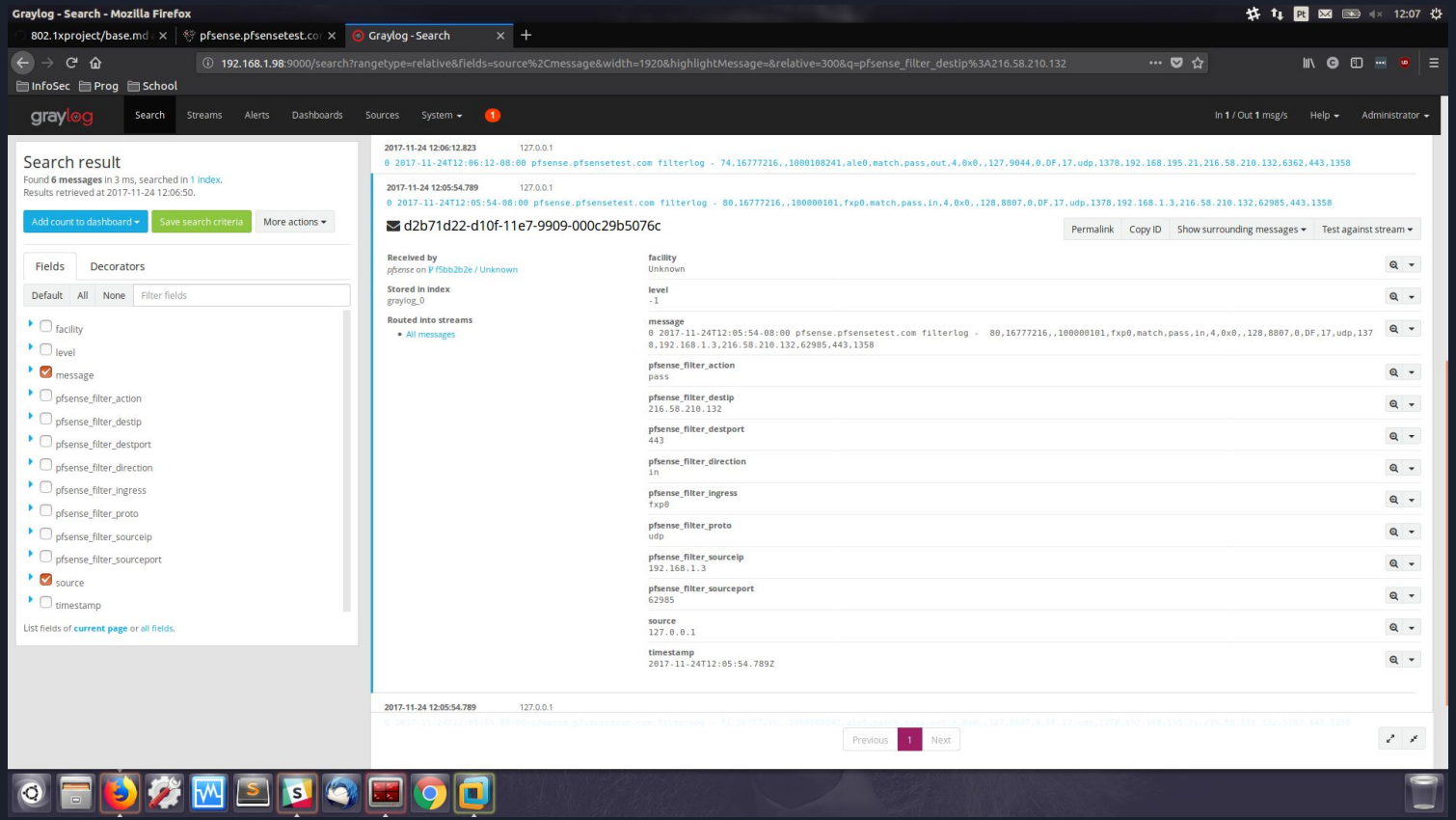
- Ativar o registo dos pacotes nas regras de firewall
  - Firewall Rules: LAN -> Source LAN -> Any (Na secção extra ativar o registo dos pacotes manipulados)
- Ativar o registo para syslog remoto: Status->System Logs-> Settings
  - Ativar o Log dos pacotes
  - Ativar o registo remoto
    - Utilizar o IP do graylog e selecionar:
      - System Events
      - Firewall Events
      - DHCP Events

Testes

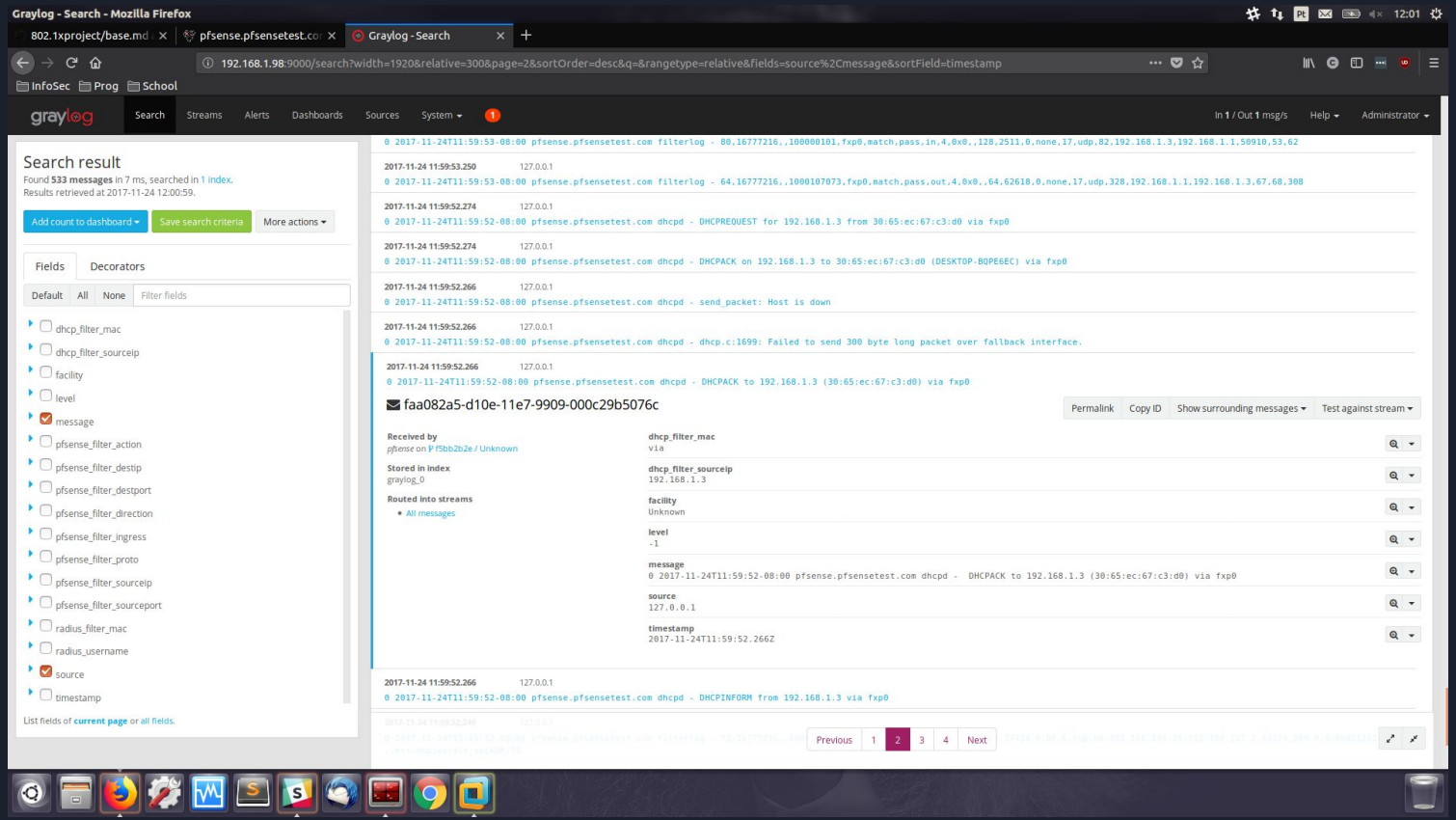
Configuramos um cliente windows para se autenticar via 802.1X



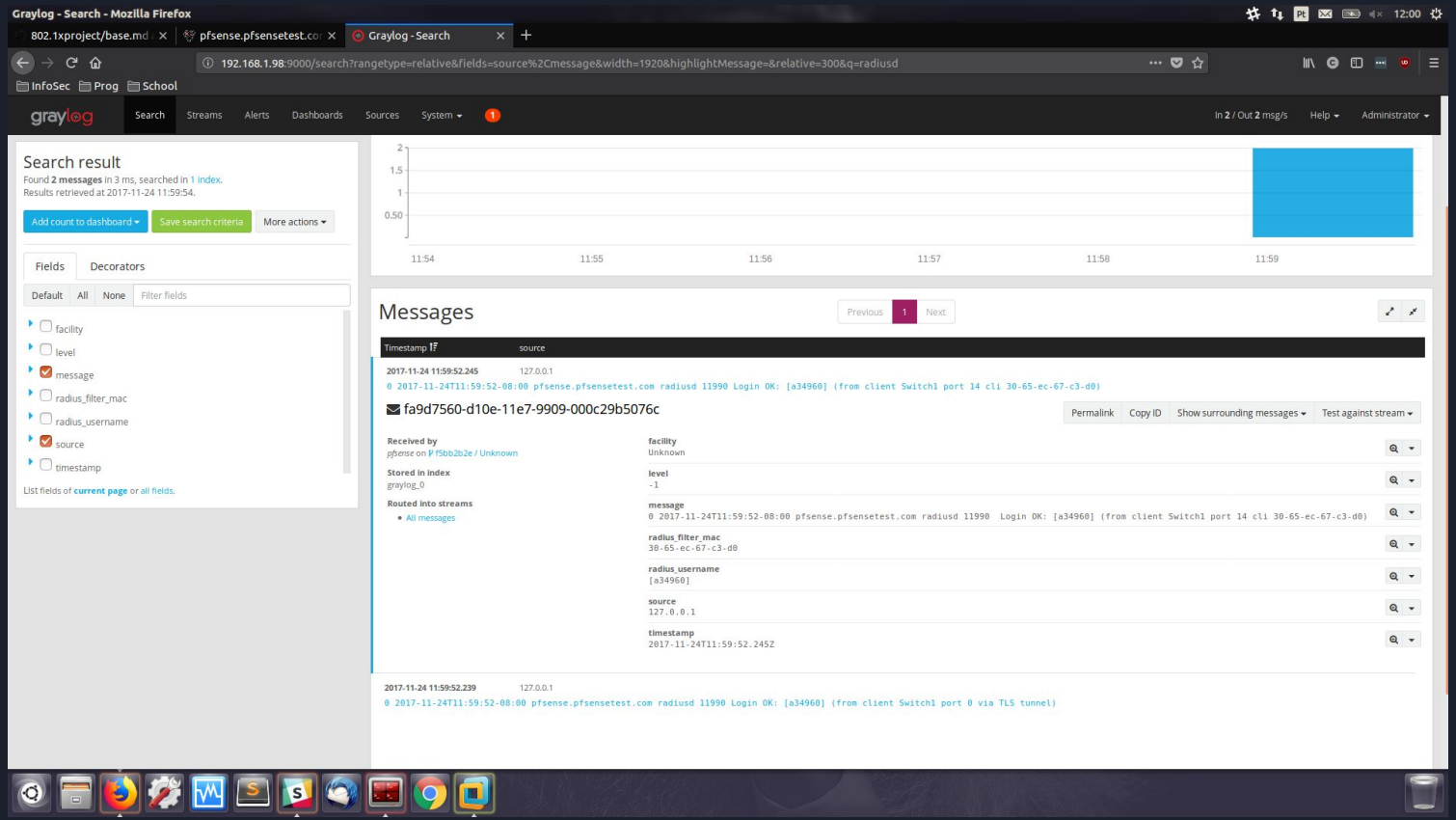



Graylog - Search - Mozilla Firefox
802.1xproject/base.md
pfsense.pfsensetest.com
Graylog - Search
192.168.1.98:9000/search?rangetype=relative&fields=source%2Cmessage&width=1920&highlightMessage=&relative=300&q=pfsense_filter_destip%3A216.58.210.132
InfoSec
Prog
School
graylog
Search
Streams
Alerts
Dashboards
Sources
System
In 1 / Out 1 msg/s
Help
Administrator
Search result
Found 6 messages in 3 ms, searched in 1 index.
Results retrieved at 2017-11-24 12:06:50.
Add count to dashboard
Save search criteria
More actions
Fields
Decorators
Default
All
None
Filter fields
facility
level
message
pfsense_filter_action
pfsense_filter_destip
pfsense_filter_destport
pfsense_filter_direction
pfsense_filter_ingress
pfsense_filter_proto
pfsense_filter_sourceip
pfsense_filter_sourceport
source
timestamp
List fields of current page or all fields.
2017-11-24 12:06:12.823 127.0.0.1
0 2017-11-24T12:06:12-08:00 pfsense.pfsensetest.com filterlog - 74,16777216,,1000108241,ale0,match,pass,out,4,0x0,,127,9044,0,DF,17,udp,1378,192.168.195.21,216.58.210.132,6362,443,1358
2017-11-24 12:05:54.789 127.0.0.1
0 2017-11-24T12:05:54-08:00 pfsense.pfsensetest.com filterlog - 80,16777216,,100000101,fxp0,match,pass,in,4,0x0,,128,8807,0,DF,17,udp,1378,192.168.1.3,216.58.210.132,62985,443,1358
d2b71d22-d10f-11e7-9909-000c29b5076c
Permalink
Copy ID
Show surrounding messages
Test against stream
Received by
pfSense on IP f5bb2b2e / Unknown
Stored in index
graylog_0
Routed into streams
All messages
facility
Unknown
level
-1
message
0 2017-11-24T12:05:54-08:00 pfsense.pfsensetest.com filterlog - 80,16777216,,100000101,fxp0,match,pass,in,4,0x0,,128,8807,0,DF,17,udp,1378,192.168.1.3,216.58.210.132,62985,443,1358
pfsense_filter_action
pass
pfsense_filter_destip
216.58.210.132
pfsense_filter_destport
443
pfsense_filter_direction
in
pfsense_filter_ingress
fxp0
pfsense_filter_proto
udp
pfsense_filter_sourceip
192.168.1.3
pfsense_filter_sourceport
62985
source
127.0.0.1
timestamp
2017-11-24T12:05:54.789Z
2017-11-24 12:05:54.789 127.0.0.1
Previous
1
Next

NAT


Graylog - Search - Mozilla Firefox
802.1xproject/base.md
pfsense.pfsensetest.com
Graylog - Search
192.168.1.98:9000/search?width=1920&relative=300&page=2&sortOrder=desc&q=&rangetype=relative&fields=source%2Cmessage&sortField=timestamp
InfoSec
Prog
School
graylog
Search
Streams
Alerts
Dashboards
Sources
System
In 1 / Out 1 msg/s
Help
Administrator
Search result
Found 533 messages in 7 ms, searched in 1 index.
Results retrieved at 2017-11-24 12:00:59.
Add count to dashboard
Save search criteria
More actions
Fields
Decorators
Default
All
None
Filter fields
dhcp_filter_mac
dhcp_filter_sourceip
facility
level
message
pfsense_filter_action
pfsense_filter_destip
pfsense_filter_destport
pfsense_filter_direction
pfsense_filter_ingress
pfsense_filter_proto
pfsense_filter_sourceip
pfsense_filter_sourceport
radius_filter_mac
radius_username
source
timestamp
List fields of current page or all fields.
0 2017-11-24T11:59:53-08:00 pfsense.pfsensetest.com filterlog - 80,16777216,,1000080101,fxp0,match,pass,in,4,0x0,,128,2511,0,none,17,udp,82,192.168.1.3,192.168.1.1,50910,53,62
2017-11-24 11:59:53.250 127.0.0.1
0 2017-11-24T11:59:53-08:00 pfsense.pfsensetest.com filterlog - 64,16777216,,1000107073,fxp0,match,pass,out,4,0x0,,64,62618,0,none,17,udp,328,192.168.1.1,192.168.1.3,67,68,308
2017-11-24 11:59:52.274 127.0.0.1
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com dhcpd - DHCPREQUEST for 192.168.1.3 from 30:65:ec:67:c3:d0 via fxp0
2017-11-24 11:59:52.274 127.0.0.1
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com dhcpd - DHCPACK on 192.168.1.3 to 30:65:ec:67:c3:d0 (DESKTOP-BQPE6EC) via fxp0
2017-11-24 11:59:52.266 127.0.0.1
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com dhcpd - send_packet: Host is down
2017-11-24 11:59:52.266 127.0.0.1
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com dhcpd - dhcp.c:1699: Failed to send 300 byte long packet over fallback interface.
2017-11-24 11:59:52.266 127.0.0.1
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com dhcpd - DHCPACK to 192.168.1.3 (30:65:ec:67:c3:d0) via fxp0
faa082a5-d10e-11e7-9909-000c29b5076c
Permalink
Copy ID
Show surrounding messages
Test against stream
Received by
pfsense on f5bb2b2e / Unknown
Stored in index
graylog_0
Routed into streams
All messages
dhcp_filter_mac
via
dhcp_filter_sourceip
192.168.1.3
facility
Unknown
level
-1
message
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com dhcpd - DHCPACK to 192.168.1.3 (30:65:ec:67:c3:d0) via fxp0
source
127.0.0.1
timestamp
2017-11-24T11:59:52.266Z
2017-11-24 11:59:52.266 127.0.0.1
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com dhcpd - DHCPINFORM from 192.168.1.3 via fxp0
Previous
1
2
3
4
Next

DHCP


Graylog - Search - Mozilla Firefox
802.1xproject/base.md
pfsense.pfsensetest.com
Graylog - Search
192.168.1.98:9000/search?rangetype=relative&fields=source%2Cmessage&width=1920&highlightMessage=&relative=300&q=radiusd
InfoSec
Prog
School
graylog
Search
Streams
Alerts
Dashboards
Sources
System
In 2 / Out 2 msg/s
Help
Administrator
Search result
Found 2 messages in 3 ms, searched in 1 index.
Results retrieved at 2017-11-24 11:59:54.
Add count to dashboard
Save search criteria
More actions
Fields
Decorators
Default
All
None
Filter fields
facility
level
message
radius_filter_mac
radius_username
source
timestamp
List fields of current page or all fields.
11:54
11:55
11:56
11:57
11:58
11:59
Messages
Previous
1
Next
Timestamp
source
2017-11-24 11:59:52.245
127.0.0.1
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com radiusd 11990 Login OK: [a34960] (from client Switch1 port 14 cli 30-65-ec-67-c3-d0)
fa9d7560-d10e-11e7-9909-000c29b5076c
Permalink
Copy ID
Show surrounding messages
Test against stream
Received by
pfsense on f5bb2b2e / Unknown
Stored in index
graylog_0
Routed into streams
All messages
facility
Unknown
level
-1
message
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com radiusd 11990 Login OK: [a34960] (from client Switch1 port 14 cli 30-65-ec-67-c3-d0)
radius_filter_mac
30-65-ec-67-c3-d0
radius_username
[a34960]
source
127.0.0.1
timestamp
2017-11-24T11:59:52.245Z
2017-11-24 11:59:52.239
127.0.0.1
0 2017-11-24T11:59:52-08:00 pfsense.pfsensetest.com radiusd 11990 Login OK: [a34960] (from client Switch1 port 0 via TLS tunnel)

Radius

Automatização para pesquisa nos logs

- Desenvolveu-se um script em python para facilitar este tipo de análise, recorrendo à API do graylog.

```
pepe@pepe-Aspire-VN7-591G:~/Documents/graylog-api-tool$ python3 graylog.py -D 40.77.226.250 -P 443 -t "2017-11-24 12:22:17.734"
Source IP : 192.168.1.99
Mac Address: 30:65:ec:67:c3:d0
Time of Login : 2017-11-24T12:18:03.386Z
Username: [a34960]
```

Conclusão e trabalho futuro

- A solução permite analisar que equipamento foi responsável por um evento que foi detectado após o source nat.
- Permite associar também ao utilizador.
- Foi desenvolvido um script para optimizar as queries ao graylog
- Integração com soluções de PFSense existentes

Futuro:

- Testes numa rede de um laboratório de informática e numa sala de informática de acesso livre
- Verificar as necessidades de espaço em disco para esta solução
- Decidir tempo de retenção e automatismos para limpar logs e afins
- Configurar uma solução com associação a vlans tendo em conta o grupo do utilizador
- Utilizar o captive portal como failover, em especial para acesso a convidados a uma rede mais restritiva

Bib & Tools

- Configuration—rsyslog 8.30.0 documentation
- pfSense Forum - link
- Welcome to the Graylog documentation —Graylog 2.3.0 documentation
- HP Pro Curve Switches 2512 and 2524 documentation
- PFsense
- Graylog
- Python