

weatherwall



Make Firewalls fun again
(and, no, they are not dead)

Pierre Chifflier <chifflier@inl.fr>

What's this ?



Schéma



NetPacket::IP

dpkg, scapy

Perl

Python

Bindings

NFQueue

Kernel (pas touche)



Le code



```
my $ip_obj = NetPacket::IP->decode($payload);  
my $record = get_city($ip_obj->{dest_ip});  
my $city = $record->city;  
my $weather = get_weather($city);  
  
if ($weather->{conditions} =~ m/[Rr]ain/  
and $city neq "Rennes")  
{  
    $payload->set_verdict($nfqueue::NF_DROP);  
    return 0;  
}  
$payload->set_verdict($nfqueue::NF_ACCEPT);
```

Le code



```
my $ip_obj = NetPacket::IP->decode($payload);  
my $record = get_record($ip_obj->{dest_ip});  
my $city = $record->{city};  
my $country = $record->{country};  
my $ip_obj->set_verdict($nfqueue::NF_DROP);  
return 0;  
}  
$payload->set_verdict($nfqueue::NF_ACCEPT);
```

Dès 2010 dans toutes les machines à voter !

Le truc sérieux

- Bindings de haut niveau sur nfqueue
- CMake, swig
- Licence GPL
- Layer7 en 10 lignes (ou presque)
- A vous de trouver

```
if ($tcp_obj->{flags} & NetPacket::TCP::PSH) {  
    if ($tcp_obj->{dport} == 80) {  
        _check_http($tcp_obj->{data})  
        or  
        return $payload->set_verdict($nfqueue::NF_DROP);  
    }  
}  
  
my @http_checks = (  
    "^GET ",  
    "^User-Agent",  
);  
  
sub _check_http  
{  
    my $data = shift;  
  
    foreach my $check (@http_checks) {  
        return 0 unless ($data =~ /$check/moi);  
    }  
  
    return 1;  
}
```

Questions ?

- NetFilter Workshop <http://workshop.netfilter.org/2008>
- Le site :
<http://software.inl.fr//trac/wiki/nfqueue-bindings>
- Wolfotrack :
<http://software.inl.fr/trac/wiki/Wolfotrack>
- Le blog : <http://www.wzdftpd.net/blog/>
- Remerciements :



Pierre Chifflier <chifflier@inl.fr>