Firewalle do zastosowań domowych

Cezary Krzyżanowski

PLD Linux Distribution
czarny@pld-linux.org

Lab. Sieci Komputerowe II, 2007

Outline

Outline

Bezpieczeństwo

- Minimum otwartych portów na na zewnątrz
- Wychwytywanie nietypowych zachowań
- Wyłapywanie cwaniactwa w sieci lokalnej
  - w szczególności WiFi

Bezpieczeństwo

- Minimum otwartych portów na na zewnątrz
- Wychwytywanie nietypowych zachowań
- Wyłapywanie cwaniactwa w sieci lokalnej
  - w szczególności WiFi

Bezpieczeństwo

- Minimum otwartych portów na na zewnątrz
- Wychwytywanie nietypowych zachowań
- Wyłapywanie cwaniactwa w sieci lokalnej
  - w szczególności WiFi

Bezpieczeństwo

- Minimum otwartych portów na na zewnątrz
- Wychwytywanie nietypowych zachowań
- Wyłapywanie cwaniactwa w sieci lokalnej
  - w szczególności WiFi

Dostępność

- Współdzielenie zasobów
  - usługi skierowane do sieci wewnętrznej
  - np. drukarki, otoczenie sieciowe, etc. . .
- Udostępnianie internetu
- Przekierowania portów

Dostępność

- Współdzielenie zasobów
  - usługi skierowane do sieci wewnętrznej
  - np. drukarki, otoczenie sieciowe, etc. . .
- Udostępnianie internetu
- Przekierowania portów

Dostępność

- Współdzielenie zasobów
  - usługi skierowane do sieci wewnętrznej
  - np. drukarki, otoczenie sieciowe, etc. . .
- Udostępnianie internetu
- Przekierowania portów

Dostępność

- Współdzielenie zasobów
  - usługi skierowane do sieci wewnętrznej
  - np. drukarki, otoczenie sieciowe, etc. . .
- Udostępnianie internetu
- Przekierowania portów

Dostępność

- Współdzielenie zasobów
  - usługi skierowane do sieci wewnętrznej
  - np. drukarki, otoczenie sieciowe, etc. . .
- Udostępnianie internetu
- Przekierowania portów

Jakość

- Płynne strumienie multimedialne
  - telefonia internetowa — Skype, SIP, etc. . .
  - multimedia WWW — Youtube, Video Google, etc. . .
  - streamcasting — radia internetowe
- Responsywna sieć WWW
- Sprawiedliwy podział łącza

Jakość

- Płynne strumienie multimedialne
  - telefonia internetowa — Skype, SIP, etc. . .
  - multimedia WWW — Youtube, Video Google, etc. . .
  - streamcasting — radia internetowe
- Responsywna sieć WWW
- Sprawiedliwy podział łącza

Jakość

- Płynne strumienie multimedialne
  - telefonia internetowa — Skype, SIP, etc...
  - multimedia WWW — Youtube, Video Google, etc...
  - streamcasting — radia internetowe
- Responsywna sieć WWW
- Sprawiedliwy podział łącza

Jakość

- Płynne strumienie multimedialne
  - telefonia internetowa — Skype, SIP, etc...
  - multimedia WWW — Youtube, Video Google, etc...
  - streamcasting — radia internetowe
- Responsywna sieć WWW
- Sprawiedliwy podział łącza

Jakość

- Płynne strumienie multimedialne
  - telefonia internetowa — Skype, SIP, etc...
  - multimedia WWW — Youtube, Video Google, etc...
  - streamcasting — radia internetowe
- Responsywna sieć WWW
- Sprawiedliwy podział łącza

Jakość

- Płynne strumienie multimedialne
  - telefonia internetowa — Skype, SIP, etc...
  - multimedia WWW — Youtube, Video Google, etc...
  - streamcasting — radia internetowe
- Responsywna sieć WWW
- Sprawiedliwy podział łącza

Outline

System operacyjny

- Linux w wersji co najmniej 2.6
- netfilter
  - iptables — tablice dla reguł wywoływane w specyficznych miejscach stosu TCP/IP
  - conntrack — przypisywanie pakietów do konkretnych połączeń
  - NAT — maskarada i przekierowanie portów
- htb — algorytm podziału łącza ze względu na przynależność do hierarchicznych klas; następca CBQ

System operacyjny

- Linux w wersji co najmniej 2.6
- netfilter
  - iptables — tablice dla reguł wywoływane w specyficznych miejscach stosu TCP/IP
  - conntrack — przypisywanie pakietów do konkretnych połączeń
  - NAT — maskarada i przekierowanie portów
- htb — algorytm podziału łącza ze względu na przynależność do hierarchicznych klas; następca CBQ

System operacyjny

- Linux w wersji co najmniej 2.6
- netfilter
  - iptables — tablice dla reguł wywoływane w specyficznych miejscach stosu TCP/IP
  - conntrack — przypisywanie pakietów do konkretnych połączeń
  - NAT — maskarada i przekierowanie portów
- htb — algorytm podziału łącza ze względu na przynależność do hierarchicznych klas; następca CBQ

System operacyjny

- Linux w wersji co najmniej 2.6
- netfilter
  - iptables — tablice dla reguł wywoływane w specyficznych miejscach stosu TCP/IP
  - conntrack — przypisywanie pakietów do konkretnych połączeń
  - NAT — maskarada i przekierowanie portów
- htb — algorytm podziału łącza ze względu na przynależność do hierarchicznych klas; następca CBQ

System operacyjny

- Linux w wersji co najmniej 2.6
- netfilter
  - iptables — tablice dla reguł wywoływane w specyficznych miejscach stosu TCP/IP
  - conntrack — przypisywanie pakietów do konkretnych połączeń
  - NAT — maskarada i przekierowanie portów
- htb — algorytm podziału łącza ze względu na przynależność do hierarchicznych klas; następca CBQ

System operacyjny

- Linux w wersji co najmniej 2.6
- netfilter
  - iptables — tablice dla reguł wywoływane w specyficznych miejscach stosu TCP/IP
  - conntrack — przypisywanie pakietów do konkretnych połączeń
  - NAT — maskarada i przekierowanie portów
- htb — algorytm podziału łącza ze względu na przynależność do hierarchicznych klas; następca CBQ

Moduły dodatkowe

- ipp2p — odnajdowanie pakietów z protokołów P2P na podstawie zawartości;
  Rozpoznawane protokoły:
  - eDonkey, eMule, Kademlia
  - KaZaA, FastTrack
  - Gnutella
  - DirectConnect
  - BitTorrent, extended BT
  - Soulseek
  - WinMX
  - AppleJuice
  - Ares, AresLite
- wrr — algorytm kolejkowania pakietów dzielący pasmo równo między wszystkie maszyny
  - sprawiedliwszy podział niż w przypadku np. sfq

Moduły dodatkowe

- ipp2p — odnajdowanie pakietów z protokołów P2P na podstawie zawartości;
  Rozpoznawane protokoły:
  - eDonkey, eMule, Kademlia
  - KaZaA, FastTrack
  - Gnutella
  - DirectConnect
  - BitTorrent, extended BT
  - Soulseek
  - WinMX
  - AppleJuice
  - Ares, AresLite
- wrr — algorytm kolejkowania pakietów dzielący pasmo równo między wszystkie maszyny
  - sprawiedliwszy podział niż w przypadku np. sfq

Moduły dodatkowe

- ipp2p — odnajdowanie pakietów z protokołów P2P na podstawie zawartości;
  Rozpoznawane protokoły:
  - eDonkey, eMule, Kademlia
  - KaZaA, FastTrack
  - Gnutella
  - DirectConnect
  - BitTorrent, extended BT
  - Soulseek
  - WinMX
  - AppleJuice
  - Ares, AresLite
- wrr — algorytm kolejkowania pakietów dzielący pasmo równo między wszystkie maszyny
  - sprawiedliwszy podział niż w przypadku np. sfq

Moduły dodatkowe

- ipp2p — odnajdowanie pakietów z protokołów P2P na podstawie zawartości;
  Rozpoznawane protokoły:
  - eDonkey, eMule, Kademlia
  - KaZaA, FastTrack
  - Gnutella
  - DirectConnect
  - BitTorrent, extended BT
  - Soulseek
  - WinMX
  - AppleJuice
  - Ares, AresLite
- wrr — algorytm kolejkowania pakietów dzielący pasmo równo między wszystkie maszyny
  - sprawiedliwszy podział niż w przypadku np. sfq

Aplikacje

- interpreter powłoki sh — firewall będzie skryptem w tej powłoce
- iptables — program do zarządzania tablicami w jądrze
- tc — program do manipulacji algorytmami kolejkowania pakietów

Aplikacje

- interpreter powłoki sh — firewall będzie skryptem w tej powłoce
- iptables — program do zarządzania tablicami w jądrze
- tc — program do manipulacji algorytmami kolejkowania pakietów

Aplikacje

- interpreter powłoki sh — firewall będzie skryptem w tej powłoce
- iptables — program do zarządzania tablicami w jądrze
- tc — program do manipulacji algorytmami kolejkowania pakietów

Outline

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - funkcje
      - specyficzne łańcuchy

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - ...
      - specyficzne łańcuchy

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - ...
      - specyficzne łańcuchy

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - ...
      - specyficzne łańcuchy

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   I. priorytetowy — VoIP, strumienie multimediów, SSH
   II. normalny — domyślny ruch (WWW, poczta, etc. . .)
   III. tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   I. priorytetowy — VoIP, strumienie multimediów, SSH
   II. normalny — domyślny ruch (WWW, poczta, etc. . .)
   III. tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   I. priorytetowy — VoIP, strumienie multimediów, SSH
   II. normalny — domyślny ruch (WWW, poczta, etc. . .)
   III. tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Ogólna struktura skryptu firewalla
Część 3

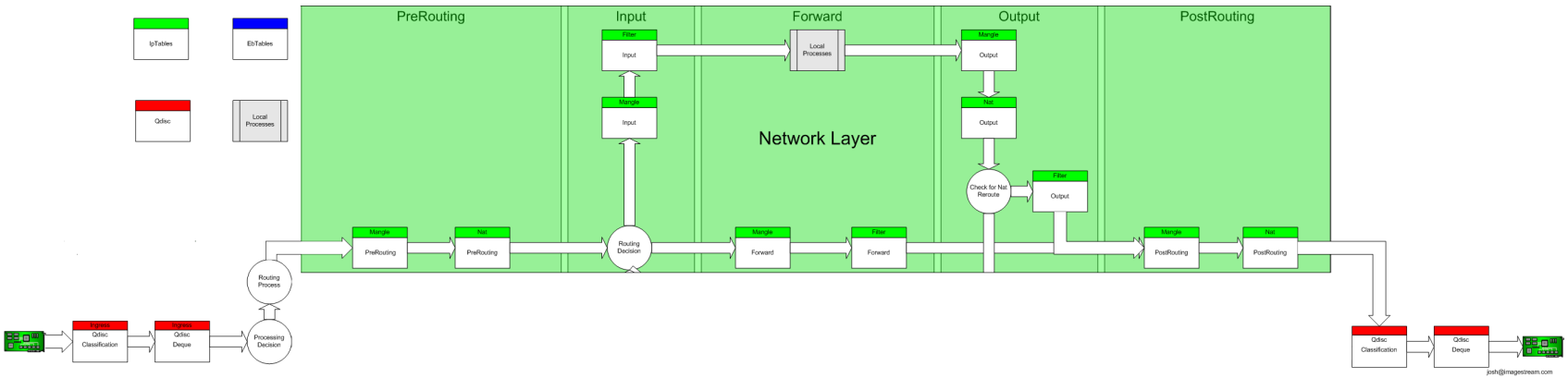
6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

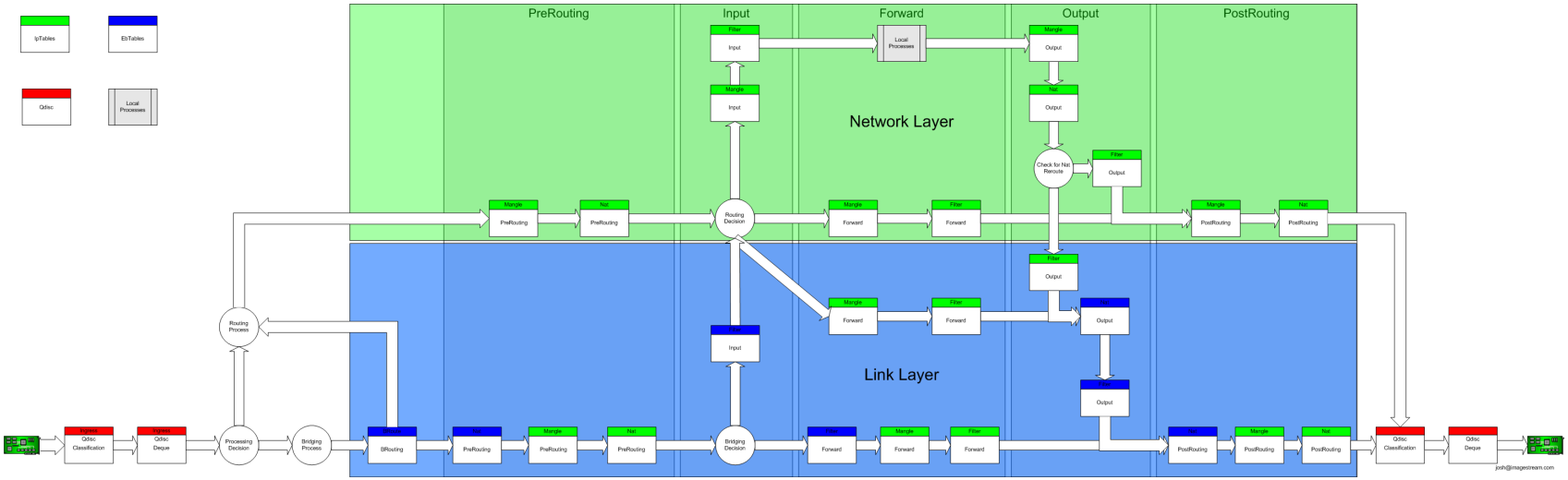
Zrozumieć iptables

Warstwa sieciowa



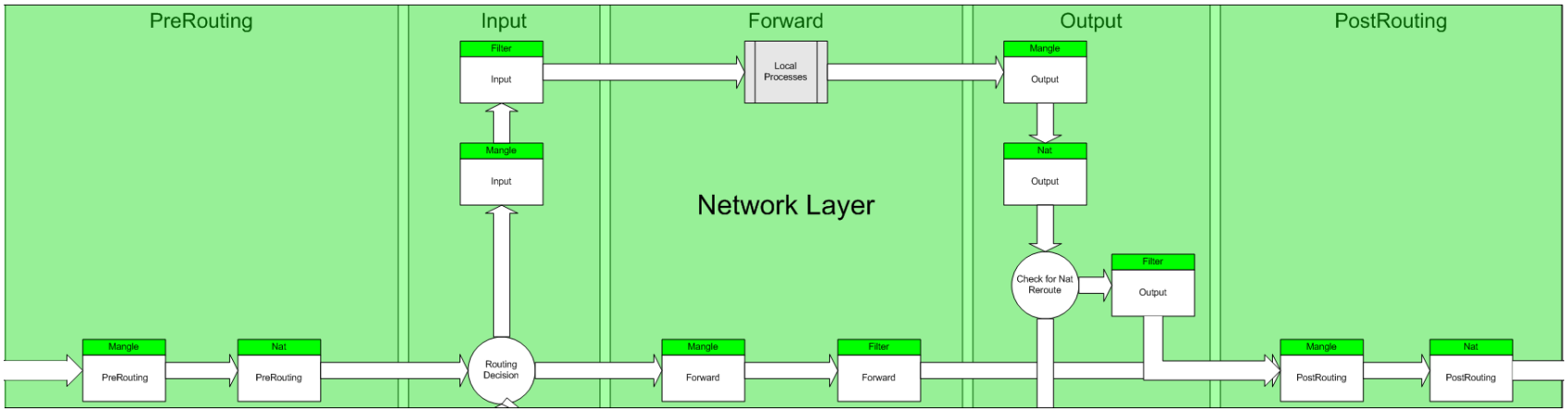
Zrozumieć iptables

Ogólny schemat przepływu pakietów



Zrozumieć iptables

Warstwa sieciowa



Outline

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzni klienci

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - ...
      - specyficzne łańcuchy

Skrypt firewalla

Ustawienia zmiennych cz. 1

Podstawowe ustawienia

Przykład

```
1 #!/bin/sh
2 PATH="/sbin:/usr/sbin:/bin:/usr/bin:${PATH}"
3 export $PATH
```

Położenie programów

Przykład

```
5 IPT="/usr/sbin/iptables"
6 MODPROBE="/sbin/modprobe"
7 TC="/sbin/tc"
```

Skrypt firewalla

Ustawienia zmiennych cz. 2

Dane konsoli dostępowej

Przykład

```
 9 REPAIR_WIFI_ADDR="192.168.0.177"
10 REPAIR_WIFI_MAC="01:23:45:67:09:AB"
11 REPAIR_LAN_ADDR="192.168.100.177"
12 REPAIR_LAN_MAC="AB:CD:EF:00:01:23"
```

Prędkości łącza

Przykład

```
14 OUTPUT_RATE=512
```

Skrypt firewalla

Ustawienia zmiennych cz. 3

Protokoły śledzone przez IPP2P

Przykład

```
16 IPP2P_MODULES="--edk --kazaa --gnu--dc --bit --apple --winmx --soul"
```

Wartości znacników

Przykład

```
18 PRIORITY_MARK=1
19 NORMAL_MARK=2
20 IPP2P_MARK=3
```

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - ...
      - specyficzne łańcuchy

Skrypt firewalla

Ustawienia zmiennych cz. 4

Deklaracje urządzeń

Przykład

```
22 INTERNET_DEV="eth1"
23 LAN_DEV="eth0"
24 WIFI_DEV="wlan0"
```

Deklaracje sieci

Przykład

```
26 LAN="192.168.100.0/24"
27 WIFI="192.168.0.0/24"
```

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - ...
      - specyficzne łańcuchy

Skrypt firewalla

Ustawienia zmiennych cz. 4

Deklaracja wykorzystywanych modułów

Przykład

```
29 MODULES=" \
30 iptable_filter \
31 iptable_mangle \
32 iptable_nat \
33 ip_tables \
34 ipt_IPMARK \
35 ipt_ipp2p \
36 ipt_MASQUERADE
37 wrr"
```

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Skrypt firewalla
Ładowanie modułów jądra

Ładowanie modułów

Przykład

```
38 for module in $MODULES; do
39         $MODPROBE $module
40 done
```

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Skrypt firewalla

Ustawianie domyślnej polityki dla tablic

Domyślna polityka dla tablic

Przykład

```
42 $IPT -P INPUT DROP
43 $IPT -P FORWARD DROP
```

Uwaga!

To jest kluczowe miejsce firewalla.
Domyślna polityka tablic to ALLOW!

Skrypt firewalla

Ustawianie domyślnej polityki dla tablic

Domyślna polityka dla tablic

Przykład

```
42 $IPT -P INPUT DROP
43 $IPT -P FORWARD DROP
```

Uwaga!

To jest kluczowe miejsce firewalla.
Domyślna polityka tablic to ALLOW!

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Skrypt firewalla

Zezwalanie na ruch po pętli zwrotnej

Dowolny ruch po pętli zwrotnej

Przykład

```
45 $IPT -A INPUT -i lo -p all -j ACCEPT
46 $IPT -A OUTPUT -o lo -p all -j ACCEPT
```

Blokowanie cwaniactw z pętlą zwrotną

Przykład

```
48 $IPT -A INPUT -p all -s localhost -i ! lo -j DROP
```

Skrypt firewalla

Zezwalanie na ruch po pętli zwrotnej

Dowolny ruch po pętli zwrotnej

Przykład

```
45 $IPT -A INPUT -i lo -p all -j ACCEPT
46 $IPT -A OUTPUT -o lo -p all -j ACCEPT
```

Blokowanie cwaniactw z pętlą zwrotną

Przykład

```
48 $IPT -A INPUT -p all -s localhost -i ! lo -j DROP
```

Ogólna struktura skryptu firewalla
Część 1

1. Ustawienia zmiennych
   - położenie programów
   - ustawienia adresów sieci i interfejsów
   - wykorzystywane moduły
2. Inicjalizacja
   1. załadowanie odpowiednich modułów
   2. ew. wyczyszczenie poprzednich ustawień
   3. zadanie domyślnych polityk
   4. ew. dodatkowe ustawienia
      - przekazywanie pakietów między interfejsami
      - tunele
      - specyficzne ścieżki

Skrypt firewalla
Uruchamianie przekazywania pakietów

Przekazywanie pakietów między interfejsami

Przykład

```
50 for dev in {$LAN_DEV,$WIFI_DEV};do
51 $IPT --append FORWARD --in-interface $dev -j ACCEPT
52 done
53 echo 1 > /proc/sys/net/ipv4/ip_forward
```

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Skrypt firewalla
Deklaracja kanału serwisowego

Bezwarunkowy dostęp dla kanału serwisowego

Przykład

```
55 $IPT -A INPUT -p all -s $REPAIR_WIFI_ADDR -i $WIFI_DEV
-m mac --mac-source $REPAIR_WIFI_MAC -j ACCEPT
56 $IPT -A INPUT -p all -s $REPAIR_LAN_ADDR -i $LAN_DEV
-m mac --mac-source $REPAIR_LAN_MAC -j ACCEPT
```

SSH zawsze włączone

Przykład

```
58 $IPT -A INPUT  -p tcp -m tcp --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
59 $IPT -A OUTPUT  -p tcp -m tcp --sport 22 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Skrypt firewalla
Deklaracja kanału serwisowego

Bezwarunkowy dostęp dla kanału serwisowego

Przykład

```
55 $IPT -A INPUT -p all -s $REPAIR_WIFI_ADDR -i $WIFI_DEV
-m mac --mac-source $REPAIR_WIFI_MAC -j ACCEPT
56 $IPT -A INPUT -p all -s $REPAIR_LAN_ADDR -i $LAN_DEV
-m mac --mac-source $REPAIR_LAN_MAC -j ACCEPT
```

SSH zawsze włączone

Przykład

```
58 $IPT -A INPUT  -p tcp -m tcp --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
59 $IPT -A OUTPUT  -p tcp -m tcp --sport 22 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Skrypt firewalla

Domyślne akceptowanie wcześniej zaakceptowanych połączeń

Twierdzenie

Nie warto skanować wszystkich pakietów z przyczyn wydajnościowych.
Lepiej szczegółowo sprawdzać pakiety nawiązujące połączenia, a te należące do już istniejących sesji przepuszczać domyślnie.

Dozwolone pakiety z już ustanowionych połączeń

Przykład

```
61 $IPT -A INPUT -m state --state
ESTABLISHED,RELATED -j ACCEPT
62 $IPT -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Skrypt firewalla

Domyślne akceptowanie wcześniej zaakceptowanych połączeń

Twierdzenie

Nie warto skanować wszystkich pakietów z przyczyn wydajnościowych.
Lepiej szczegółowo sprawdzać pakiety nawiązujące połączenia, a te należące do już istniejących sesji przepuszczać domyślnie.

Dozwolone pakiety z już ustanowionych połączeń

Przykład

```
61 $IPT -A INPUT -m state --state
ESTABLISHED,RELATED -j ACCEPT
62 $IPT -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Skrypt firewalla
Usługi sieci wewnętrznej

Osobna tablica dla usług w sieci wewnętrznej

Przykład

```
64 $IPT -N INNER_SERVICES
65 for dev in {$WIFI_DEV,$LAN_DEV}; do
66 $IPT -A INPUT -i $dev -m state --state
NEW,ESTABLISHED -j INNER_SERVICES
67  $IPT -A INPUT -i $dev -m state --state
NEW,ESTABLISHED -j RETURN
68 done
```

Skrypt firewalla
Usługi sieci wewnętrznej cz.2

Twierdzenie

Zwykle nie ma potrzeby ograniczać sieci wewnętrznej dla potrzeb domowych.

Dopuszczanie wszystkich pakietów z tablicy usług wewnętrznych

Przykład

```
70 $IPT -A INNER_SERVICES -j ACCEPT
```

Skrypt firewalla

Usługi sieci wewnętrznej cz.2

Twierdzenie

Zwykle nie ma potrzeby ograniczać sieci wewnętrznej dla potrzeb domowych.

Dopuszczanie wszystkich pakietów z tablicy usług wewnętrznych

Przykład

```
70 $IPT -A INNER_SERVICES -j ACCEPT
```

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Skrypt firewalla
Usługi sieci zewnętrznej

Twierdzenie

Osobna tablica dla usług zewnętrznych przyspieszy proces filtrowania.

Osobna tablica dla usług zewnętrznych

Przykład

```
72 $IPT -N ALLOWED_SERVICES
73 $IPT -A INPUT -i $INTERNET_DEV -m state --state
NEW -j ALLOWED_SERVICES
```

Skrypt firewalla
Usługi sieci zewnętrznej

Twierdzenie

Osobna tablica dla usług zewnętrznych przyspieszy proces filtrowania.

Osobna tablica dla usług zewnętrznych

Przykład

```
72 $IPT -N ALLOWED_SERVICES
73 $IPT -A INPUT -i $INTERNET_DEV -m state --state
NEW -j ALLOWED_SERVICES
```

Skrypt firewalla

Usługi sieci zewnętrznej cz.2

Przykład (Otwarcie portów dla BitTorrenta)

```
 75 $IPT -A ALLOWED_SERVICES -p tcp -m tcp --dport
6881 -j ACCEPT
 76 $IPT -A ALLOWED_SERVICES -p udp -m udp --dport
6881 -j ACCEPT
 77 $IPT -A ALLOWED_SERVICES -p tcp -m tcp --dport
6882 -j ACCEPT
 78 $IPT -A ALLOWED_SERVICES -p udp -m udp --dport
6882 -j ACCEPT
```

Skrypt firewalla

Usługi sieci zewnętrznej cz.2

Przykład (Otwarcie portów dla BitTorrenta - wersja krótsza)

```
 75 $IPT -A ALLOWED_SERVICES -p tcp -m tcp -m mport
--dports 6881-6882 -j ACCEPT
 76 $IPT -A ALLOWED_SERVICES -p udp -m udp -m mport
--dports 6881-6882 -j ACCEPT
```

Ogólna struktura skryptu firewalla
Część 2

3. Serwisowy kanał dostępowy
   - konkretny interfejs
   - konkretna sieć
   - konkretny adres IP
   - konkretny fizyczny MAC
   - konkretne usługi
   - ew. inne cechy
4. Specyfikacja dozwolonych usług
   - dla sieci wewnętrznej (zaufanej)
   - dla sieci zewnętrznej (niebezpiecznej)
5. Ew. przekierowania portów

Skrypt firewalla
Maskarada ruchu wychodzącego

Maskarada

Przykład

```
78 for net in {$LAN,$WIFI}; do
79 $IPT -t nat -A POSTROUTING -o $INTERNET_DEV -s $net -j  MASQUERADE
80 done
```

Skrypt firewalla
Przekierowywanie portów

Przekierowanie portów dla telefonii internetowej

Przykład (Ekiga — TCP)

```
82 for addr in {$KACPER_WIFI_ADDR,$KACPER_LAN_ADDR}; do
83 $IPT -t nat -A PREROUTING -p tcp -m tcp -i $INTERNET_DEV --dport 1720 -j DNAT --to-destination $addr
84 done
```

Przykład (Ekiga — UDP)

```
86 for addr in {$KACPER_WIFI_ADDR,$KACPER_LAN_ADDR}; do
87 $IPT -t nat -A PREROUTING -p udp -m udp -m multiport -i $INTERNET_DEV --dports 5062,5060 -j DNAT --to-destination $addr
88 done
```

Skrypt firewalla
Przekierowywanie portów

Przekierowanie portów dla telefonii internetowej

Przykład (Ekiga — TCP)

```
82 for addr in {$KACPER_WIFI_ADDR,$KACPER_LAN_ADDR};
do
83 $IPT -t nat -A PREROUTING -p tcp -m tcp -i
$INTERNET_DEV --dport 1720 -j DNAT --to-destination $addr
84 done
```

Przykład (Ekiga — UDP)

```
86 for addr in {$KACPER_WIFI_ADDR,$KACPER_LAN_ADDR};
do
87 $IPT -t nat -A PREROUTING -p udp -m udp -m multiport -i
$INTERNET_DEV --dports 5062,5060 -j DNAT --to-destination $addr
88 done
```

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   I. priorytetowy — VoIP, strumienie multimediów, SSH
   II. normalny — domyślny ruch (WWW, poczta, etc. . .)
   III. tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Skrypt firewalla
Znacznikowanie

Odzyskanie znacznika dla pakietów innych niż NEW/ESTABLISHED i uniknięcie podwójnego znacznikowania

Przykład

```
90 for chain in {PREROUTING,OUTPUT}; do
91 $IPT -t mangle -A $chain -j CONNMARK --restore-mark
92  $IPT -t mangle -A $chain -m mark ! --mark 0 -j ACCEPT
93 done
```

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   I. priorytetowy — VoIP, strumienie multimediów, SSH
   II. normalny — domyślny ruch (WWW, poczta, etc. . .)
   III. tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Skrypt firewalla
Znacznikowanie cz.2

Twierdzenie

Główne znaczenie dla responsywności sieci mają pakiety ustanowienia połączeń (flagi SYN, ACK, RST) i zgłaszania błędów (protokół ICMP)

Przykład (Znaczenie ruchu priorytetowego)

```
95 for chain in {PREROUTING,OUTPUT}; do
96 $IPT -t mangle -A $chain -p icmp -j MARK --set-mark $PRIORITY_MARK
97 $IPT -t mangle -A $chain -p tcp -m tcp --tcp-flags SYN,RST,ACK SYN -j MARK --set-mark $PRIORITY_MARK
98 $IPT -t mangle -A $chain -p tcp -m tcp --dport 22 -j MARK --set-mark $PRIORITY_MARK
99 done
```

Skrypt firewalla
Znacznikowanie cz.2

Twierdzenie

Główne znaczenie dla responsywności sieci mają pakiety ustanowienia połączeń (flagi SYN, ACK, RST) i zgłaszania błędów (protokół ICMP)

Przykład (Znaczenie ruchu priorytetowego)

```
95 for chain in {PREROUTING,OUTPUT}; do
96 $IPT -t mangle -A $chain -p icmp -j MARK --set-mark $PRIORITY_MARK
97 $IPT -t mangle -A $chain -p tcp -m tcp --tcp-flags SYN,RST,ACK SYN -j MARK --set-mark $PRIORITY_MARK
98 $IPT -t mangle -A $chain -p tcp -m tcp --dport 22 -j MARK --set-mark $PRIORITY_MARK
99 done
```

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Skrypt firewalla
Znacznikowanie cz.3

Znacznikowanie ruchu P2P

Przykład

```
101 for chain in {PREROUTING,OUTPUT}; do
102 $IPT -t mangle -A $chain -m ipp2p $IPP2P_MODULES -j MARK --set-mark $IPP2P_MARK
103 # connection tracking
104 $IPT -t mangle -A $chain -m mark --mark $IPP2P_MARK -j CONNMARK --save-mark
105 done
```

Skrypt firewalla
Znacznzikowanie cz.4

Pytanie

Dlaczego nie znaczyliśmy ruchu domyślnego?

Odpowiedź

Gdyż na podstawie wykluczenia cały pozostały ruch można skierować do klasy domyślnej.

Obserwacja

Podejście takie daje znaczny zysk wydajnościowy.

Skrypt firewalla
Znacznzikowanie cz.4

Pytanie

Dlaczego nie znaczyliśmy ruchu domyślnego?

Odpowiedź

Gdyż na podstawie wykluczenia cały pozostały ruch można skierować do klasy domyślnej.

Obserwacja

Podejście takie daje znaczny zysk wydajnościowy.

Skrypt firewalla
Znacznzikowanie cz.4

Pytanie

Dlaczego nie znaczyliśmy ruchu domyślnego?

Odpowiedź

Gdyż na podstawie wykluczenia cały pozostały ruch można skierować do klasy domyślnej.

Obserwacja

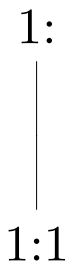
Podejście takie daje znaczny zysk wydajnościowy.

Graficzna reprezentacja klas ruchu

1:

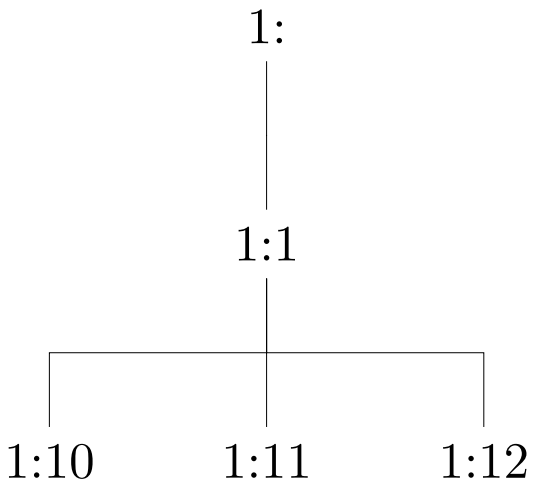
- Karta sieciowa
- HTB jako główna klasa kolejkowania
- Trzy podklasy dla trzech typów ruchu
- Właściwe kolejki

Graficzna reprezentacja klas ruchu



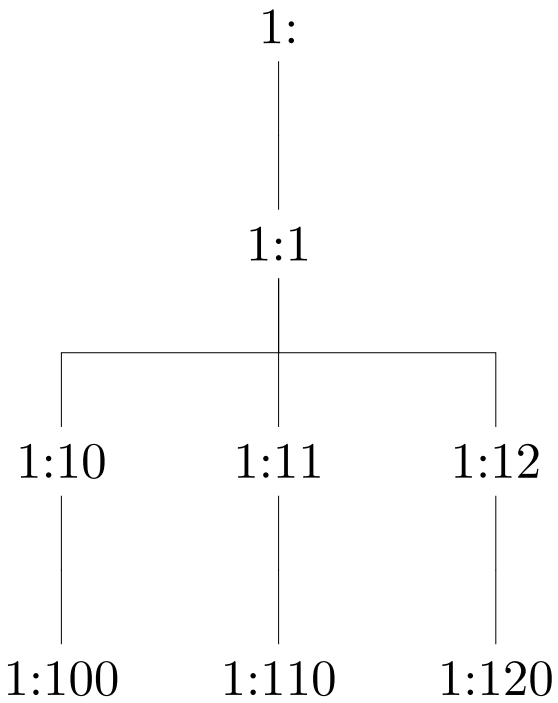
- Karta sieciowa
- HTB jako główna klasa kolejkowania
- Trzy podklasy dla trzech typów ruchu
- Właściwe kolejki

Graficzna reprezentacja klas ruchu



- Karta sieciowa
- HTB jako główna klasa kolejkowania
- Trzy podklasy dla trzech typów ruchu
- Właściwe kolejki

Graficzna reprezentacja klas ruchu



- Karta sieciowa
- HTB jako główna klasa kolejkowania
- Trzy podklasy dla trzech typów ruchu
- Właściwe kolejki

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Skrypt firewalla
Konfigurowanie klas ruchu

Podpięcie HTB jako zarządcy dla interfejsu.

Przykład

```
107 $TC qdisc add dev $INTERNET_DEV root handle 1: htb default 11
```

Graficzna reprezentacja klas ruchu

1:

- Karta sieciowa
- HTB jako główna klasa kolejkowania
- Trzy podklasy dla trzech typów ruchu
- Właściwe kolejki

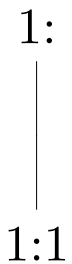
Skrypt firewalla
Konfigurowanie klas ruchu

Podpięcie HTB jako zarządcy dla interfejsu.

Przykład

```
107 $TC qdisc add dev $INTERNET_DEV root handle 1: htb default 11
```

Graficzna reprezentacja klas ruchu



- Karta sieciowa
- HTB jako główna klasa kolejkowania
- Trzy podklasy dla trzech typów ruchu
- Właściwe kolejki

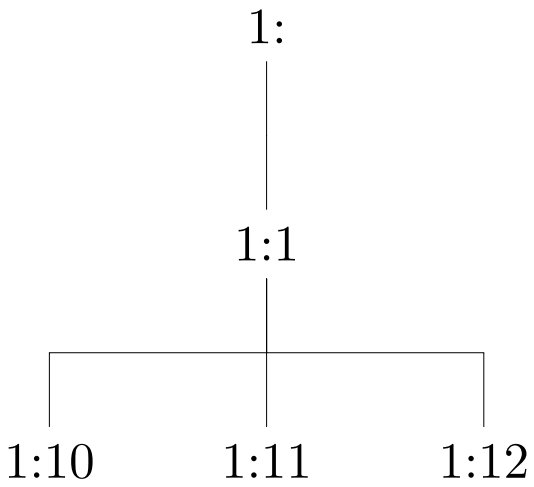
Skrypt firewalla
Konfigurowanie klas ruchu cz.2

Podpięcie HTB jako zarządcy dla interfejsu.

Przykład

```
109 $TC class add dev $INTERNET_DEV parent 1: classid
1:1 htb rate $(($OUTPUT_RATE - 20))kbit ceil
$(($OUTPUT_RATE - 20))kbit
```

Graficzna reprezentacja klas ruchu



- Karta sieciowa
- HTB jako główna klasa kolejkowania
- Trzy podklasy dla trzech typów ruchu
- Właściwe kolejki

Skrypt firewalla
Konfigurowanie klas ruchu cz.3

Trzy klasy dla trzech rodzajów ruchu.

Przykład (Klasa priorytetowa)

111 $TC class add dev $INTERNET_DEV parent 1:1 classid 1:10 htb rate 100kbit ceil 100kbit prio 1 burst 2k

Pytanie

Dlaczego dajemy klasie priorytetowej tylko 100kb/s z 512kb/s dostępnych łącza?

Odpowiedź

W ten sposób zabilibyśmy właściwą komunikacje na rzecz sygnalizacji.

Skrypt firewalla
Konfigurowanie klas ruchu cz.3

Trzy klasy dla trzech rodzajów ruchu.

Przykład (Klasa priorytetowa)

111 $TC class add dev $INTERNET_DEV parent 1:1 classid 1:10 htb rate 100kbit ceil 100kbit prio 1 burst 2k

Pytanie

Dlaczego dajemy klasie priorytetowej tylko 100kb/s z 512kb/s dostępnych łącza?

Odpowiedź

W ten sposób zabilibyśmy właściwą komunikacje na rzecz sygnalizacji.

Skrypt firewalla
Konfigurowanie klas ruchu cz.3

Trzy klasy dla trzech rodzajów ruchu.

Przykład (Klasa priorytetowa)

111 $TC class add dev $INTERNET_DEV parent 1:1 classid 1:10 htb rate 100kbit ceil 100kbit prio 1 burst 2k

Pytanie

Dlaczego dajemy klasie priorytetowej tylko 100kb/s z 512kb/s dostępnych łącza?

Odpowiedź

W ten sposób zabilibyśmy właściwą komunikacje na rzecz sygnalizacji.

Skrypt firewalla
Konfigurowanie klas ruchu cz.4

Przykład (Klasa domyślna)

```
113 $TC class add dev $INTERNET_DEV parent 1:1 classid
1:11 htb rate 300kbit ceil $(($OUTPUT_RATE -20))kbit prio 2
burst 2k
```

Przykład (Klasa P2P)

```
115 $TC class add dev $INTERNET_DEV parent 1:1 classid
1:12 htb rate 100kbit ceil $(($OUTPUT_RATE - 20))kbit prio 3
```

Skrypt firewalla

Konfigurowanie klas ruchu cz.4

Przykład (Klasa domyślna)

```
113 $TC class add dev $INTERNET_DEV parent 1:1 classid
1:11 htb rate 300kbit ceil $(($OUTPUT_RATE -20))kbit prio 2
burst 2k
```

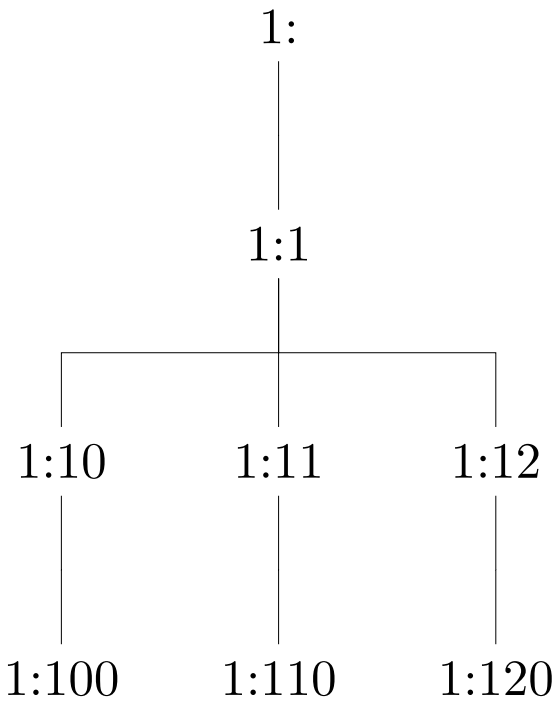
Przykład (Klasa P2P)

```
115 $TC class add dev $INTERNET_DEV parent 1:1 classid
1:12 htb rate 100kbit ceil $(($OUTPUT_RATE - 20))kbit prio 3
```

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Graficzna reprezentacja klas ruchu



- Karta sieciowa
- HTB jako główna klasa kolejkowania
- Trzy podklasy dla trzech typów ruchu
- Właściwe kolejki

Skrypt firewalla
Algorytmy kolejkowania

Właściwe algorytmy kolejkowania

Przykład

```
117 $TC qdisc add dev $INTERNET_DEV parent 1:10 handle
100: wrr sour ip 20 0
118 $TC qdisc add dev $INTERNET_DEV parent 1:11 handle
110: wrr sour ip 20 0
119 $TC qdisc add dev $INTERNET_DEV parent 1:12 handle
120: wrr sour ip 20 0
```

Ogólna struktura skryptu firewalla
Część 3

6. Znacznikowanie pakietów
   - I priorytetowy — VoIP, strumienie multimediów, SSH
   - II normalny — domyślny ruch (WWW, poczta, etc. . .)
   - III tło — P2P
7. Definicja klas ruchu
   1. 3 klasy główne dla 3 rodzajów ruchu
   2. Algorytmy kolejkowania dla poszczególnych klas
   3. Filtry przydzielające pakiety do klas na podstawie znaczników

Skrypt firewalla
Filtry przydzielające pakiety do klas

Definiowanie filtrów przydziału pakietów do klas

Przykład (Ruch priorytetowy)

```
121 $TC filter add dev $INTERNET_DEV parent 1:0 protocol
ip prio 1 handle 1 fw class 1:10
```

Przykład (Ruch domyślny)

```
122 $TC filter add dev $INTERNET_DEV parent 1:0 protocol
ip prio 2 handle 2 fw class 1:11
```

Przykład (Ruch P2P)

```
123 $TC filter add dev $INTERNET_DEV parent 1:0 protocol
ip prio 3 handle 3 fw class 1:12
```

Skrypt firewalla

Filtry przydzielające pakiety do klas

Definiowanie filtrów przydziału pakietów do klas

Przykład (Ruch priorytetowy)

```
121 $TC filter add dev $INTERNET_DEV parent 1:0 protocol
ip prio 1 handle 1 fw class 1:10
```

Przykład (Ruch domyślny)

```
122 $TC filter add dev $INTERNET_DEV parent 1:0 protocol
ip prio 2 handle 2 fw class 1:11
```

Przykład (Ruch P2P)

```
123 $TC filter add dev $INTERNET_DEV parent 1:0 protocol
ip prio 3 handle 3 fw class 1:12
```

Skrypt firewalla

Filtry przydzielające pakiety do klas

Definiowanie filtrów przydziału pakietów do klas

Przykład (Ruch priorytetowy)

```
121 $TC filter add dev $INTERNET_DEV parent 1:0 protocol
ip prio 1 handle 1 fw class 1:10
```

Przykład (Ruch domyślny)

```
122 $TC filter add dev $INTERNET_DEV parent 1:0 protocol
ip prio 2 handle 2 fw class 1:11
```

Przykład (Ruch P2P)

```
123 $TC filter add dev $INTERNET_DEV parent 1:0 protocol
ip prio 3 handle 3 fw class 1:12
```

Podsumowanie

- Automagiczny firewall nigdy nie zadziała.
- Domyślna polityka DROP na wszystkich tablicach.
- Warto stawiać zewnętrzne firewalle na brzegach sieci domowych, choćby ze względów wydajnościowych.

- Outlook
  - Something you haven't solved.
  - Something else you haven't solved.