

Kontrola dostępu w środowiskach heterogenicznych

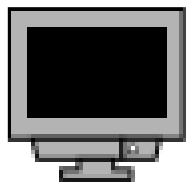


1. Składniki
2. Sieć
3. Autentykacja a autoryzacja
4. Autentykacja
5. Autoryzacja
6. Przebieg połączenia
7. Uwagi
8. Działający przykład
9. Czas na pytania
10. Zakończenie

Kontrola dostępu w środowiskach heterogenicznych



- 1. Składniki
- 1.1 Klient



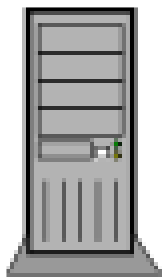
klient

Pracujemy w sieci heterogenicznej - maszyny klienckie znajdują się pod kontrolą naszego ulubionego "systemu operacyjnego" - Microsoft (tm)(r)(c)(whatever) Windows (tm)(c)(r)(whatever).

Kontrola dostępu w środowiskach heterogenicznych



- 1. Składniki
- 1.2 Serwer



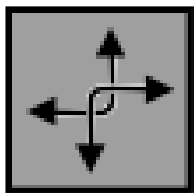
serwer

Serwer autentykacyjny i plików - działający pod kontrolą dowolnej dystrybucji GNU/Linux z Sambą.

Kontrola dostępu w środowiskach heterogenicznych



- 1. Składniki
- 1.3 Router



bramka

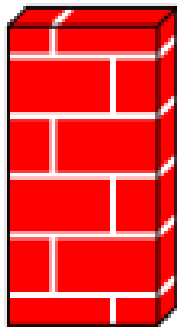
Nasz router, niezależnie od tego, przez jaki system operacyjny kontrolowany, musi posiadać typowo firewallową opcję - możliwość DNATowania i SNATowania.

Kontrola dostępu w środowiskach heterogenicznych



1. Składniki

1.4 Most



transparent

Centralny punkt systemu kontroli dostępu - most z filtrującym proxy i firewallem. Aby posiadał on pełną funkcjonalność, filtrujący proxy musi mieć możliwość przydzielania różnych regułek dla różnych źródłowych adresów IP.

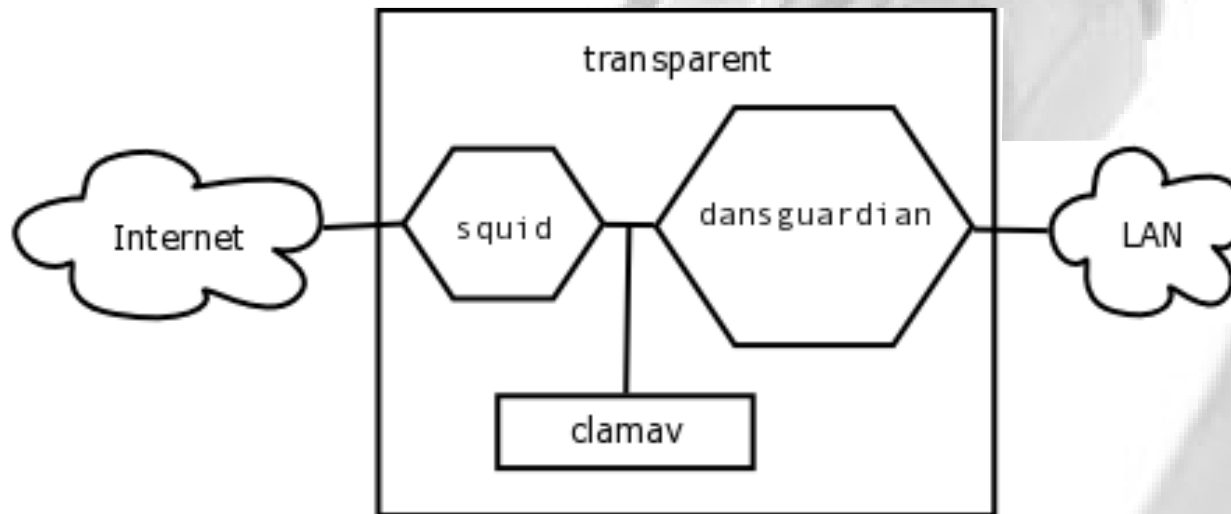
Kontrola dostępu w środowiskach heterogenicznych



1. Składniki

1.4 Most

1.4.1 Oprogramowanie mostu



Oprogramowanie mostu to buforujący serwer proxy, filtrujący serwer proxy, antywirus i odpowiedni firewall.

Kontrola dostępu w środowiskach heterogenicznych



- 1. Składniki
- 1.5 Zdalny host



zdalny host

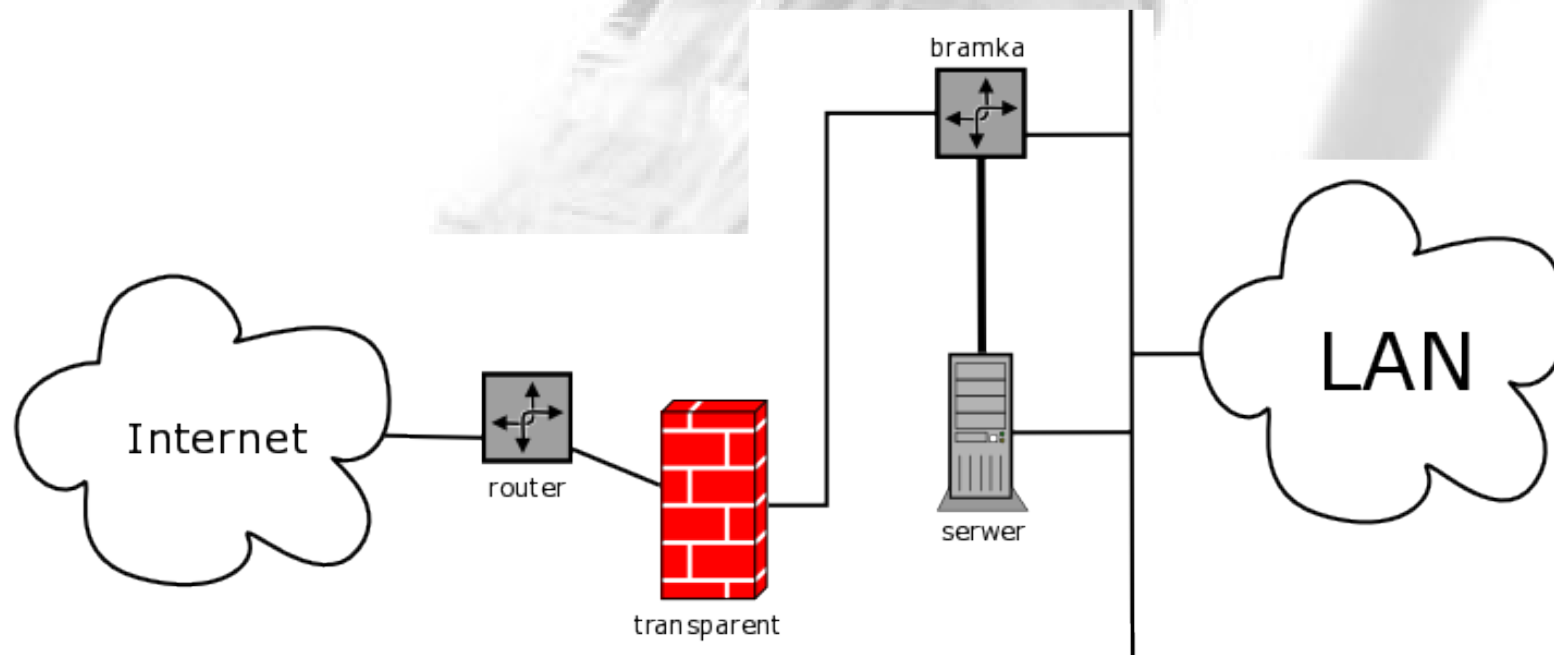
www.BardzoBrzydkaStrona.com

Zdalny host, który będzie nam służył do testowania (głównie filtrującego proxy). Powinien być to serwis WWW, którego treść będzie dozwolona dla jednej grupy klientów podczas, gdy inna ich grupa nie powinna mieć do niego dostępu.

Kontrola dostępu w środowiskach heterogenicznych



2. Sieć



Kontrola dostępu w środowiskach heterogenicznych



3. Autentykacja a autoryzacja



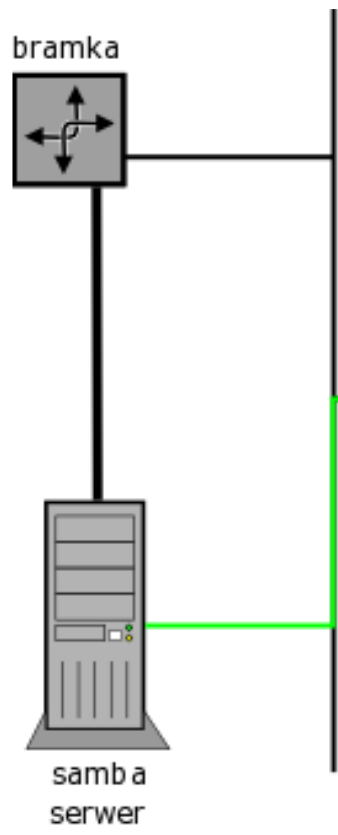
Autentykacja - proces sprawdzenia, czy zadeklarowana tożsamość zgodna jest z rzeczywistością.

Autoryzacja - proces sprawdzenia, czy zautentykowany użytkownik ma dostęp do zasobów, do których dostęp chce uzyskać.

Kontrola dostępu w środowiskach heterogenicznych



4. Autentykacja 4.1 Proces

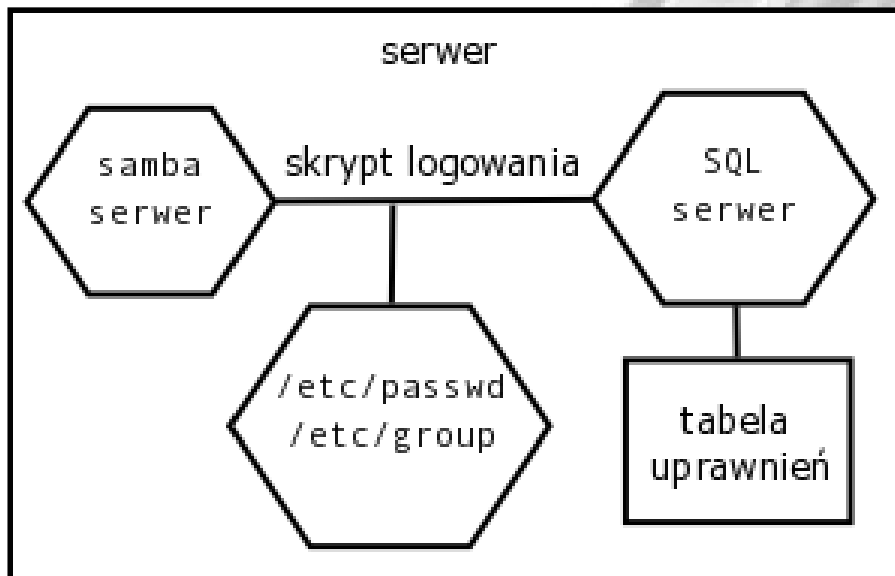


Klient autentkuje się bezpośrednio do serwera autentykacyjnego działającego na Sambie. Ten natomiast przydziela klientowi domyślną politykę.

Kontrola dostępu w środowiskach heterogenicznych



4. Autentykacja 4.2 Rozpoznawanie użytkownika



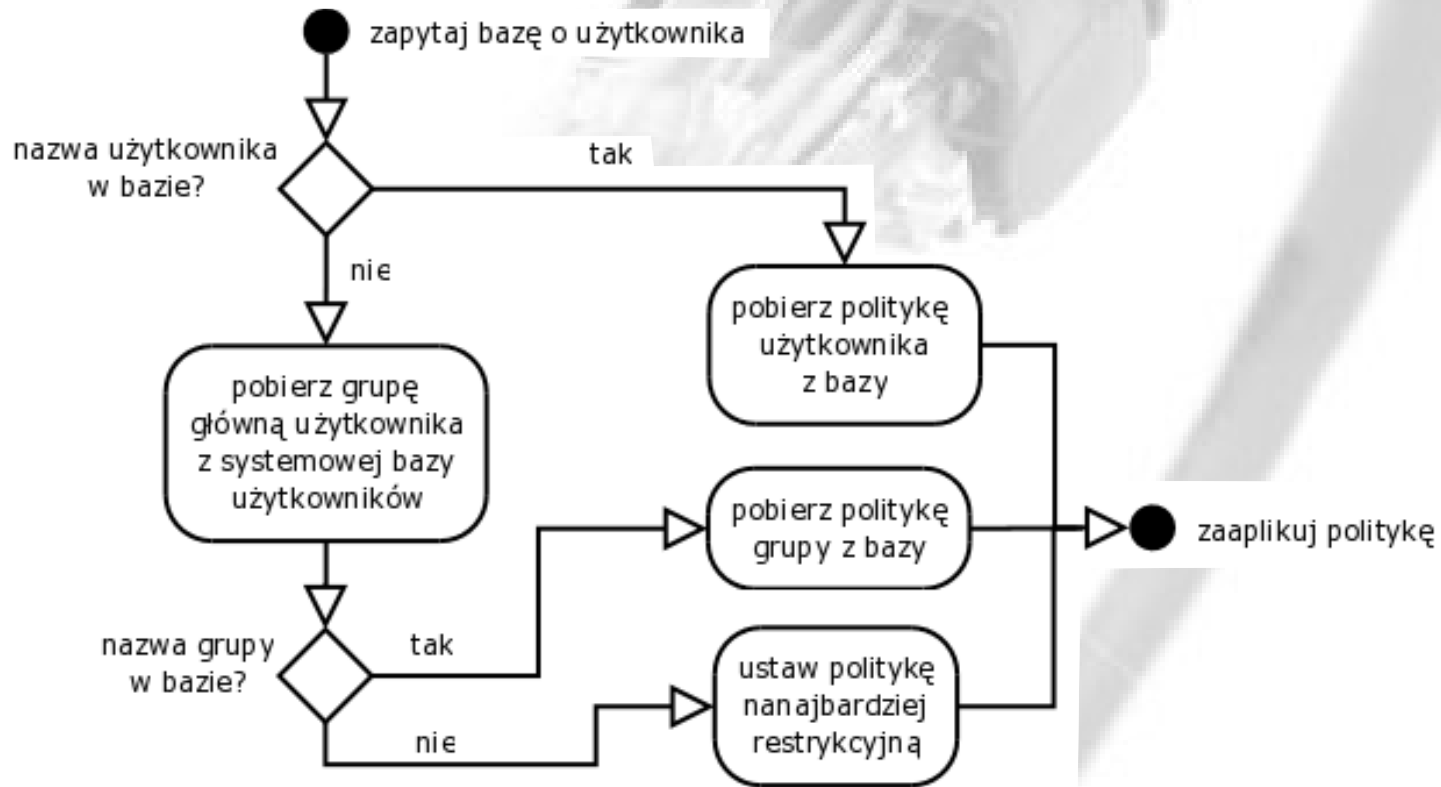
Serwer samby poprzez skrypt logowania komunikuje się z bazą danych zawierającą polityki dla użytkowników oraz z systemową bazą użytkowników.

Kontrola dostępu w środowiskach heterogenicznych



4. Autentykacja

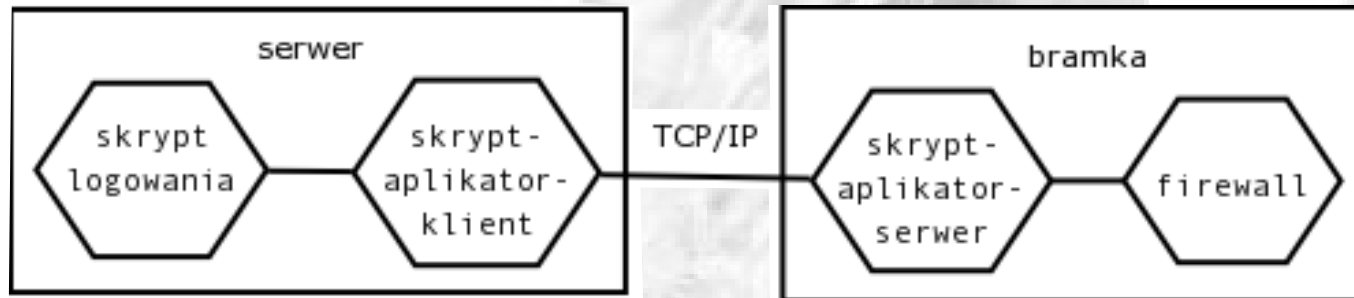
4.2 Rozpoznawanie użytkownika (c.d.)



Kontrola dostępu w środowiskach heterogenicznych



4. Autentykacja 4.3 Aplikowanie domyślnej polityki



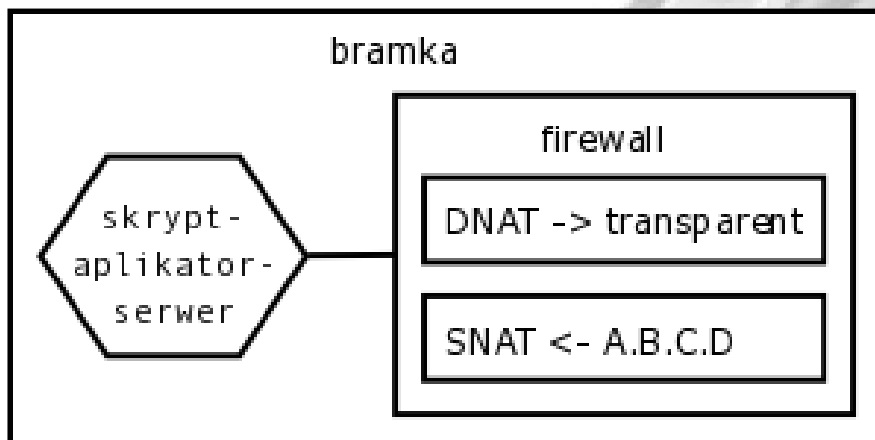
Skrypt logowania uruchamia skrypt-aplikator polityki, który łączy się ze swoim drugim końcem na routerze i ustawia odpowiednie wpisy w firewallu.

Kontrola dostępu w środowiskach heterogenicznych



5. Autoryzacja

5.1 Aplikowanie reguł polityki

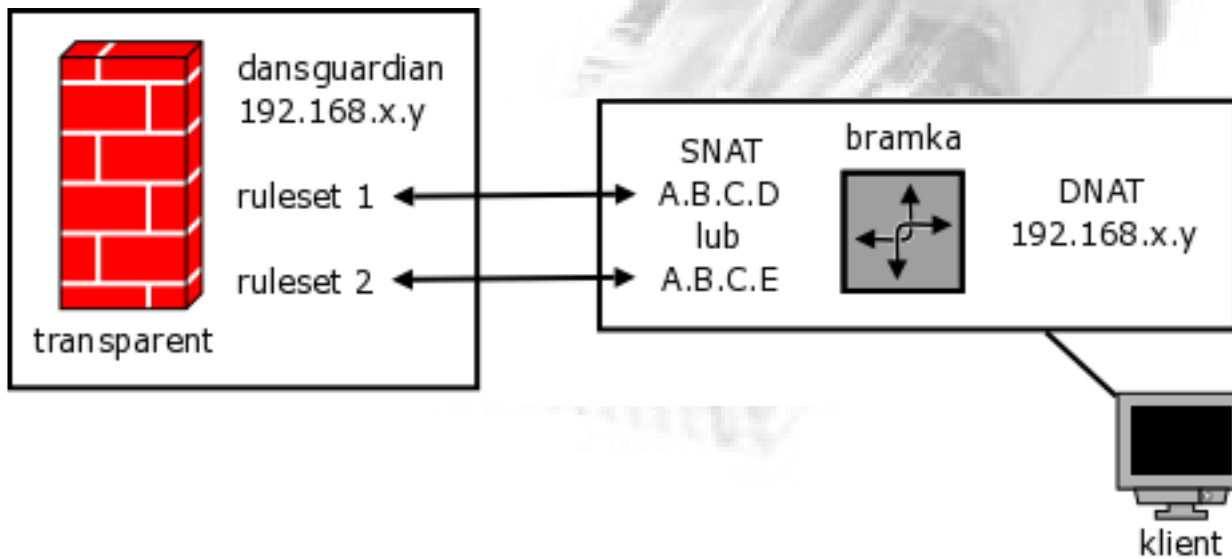


Skrypt-aplikator ustawia w firewallu odpowiednie reguły zapewniające kierowanie żądań do serwera proxy i ustawiające odpowiedni adres źródłowy.

Kontrola dostępu w środowiskach heterogenicznych



5. Autoryzacja 5.2 Aplikowanie zestawów filtrów

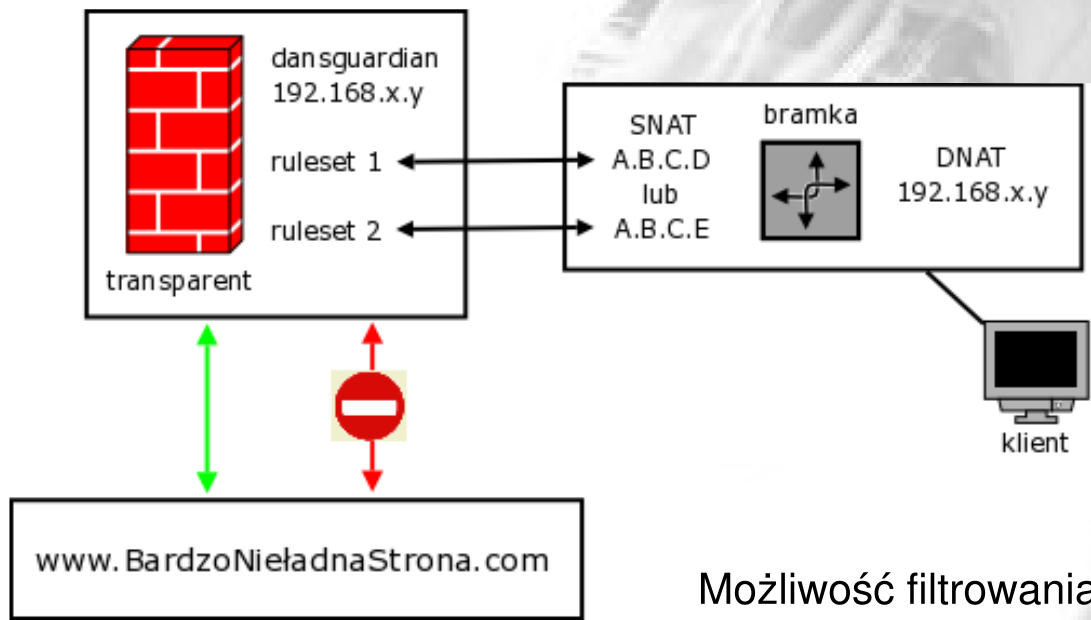


Filtrujący serwer proxy aplikuje zestaw filtrów w zależności od tego, z jakiego adresu IP przychodzi żądanie HTTP.

Kontrola dostępu w środowiskach heterogenicznych



- 5. Autoryzacja
- 5.3 Rodzaje filtrów
- 5.3.1 Filtrowanie adresów

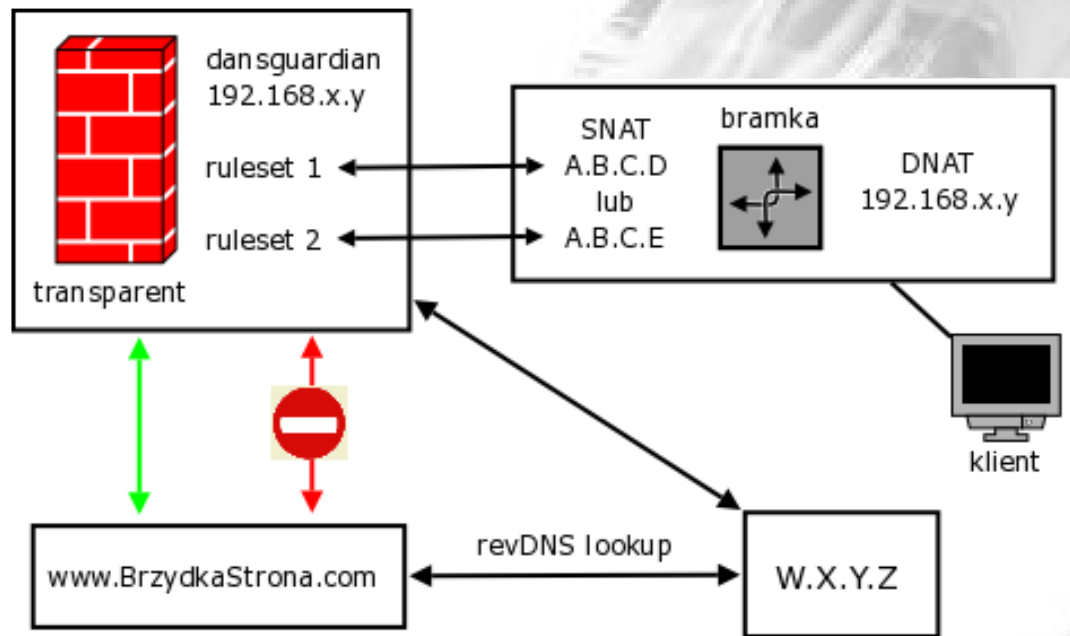


Możliwość filtrowania po adresach URL.

Kontrola dostępu w środowiskach heterogenicznych



- 5. Autoryzacja
- 5.3 Rodzaje filtrów
- 5.3.2 Odwrotny DNS

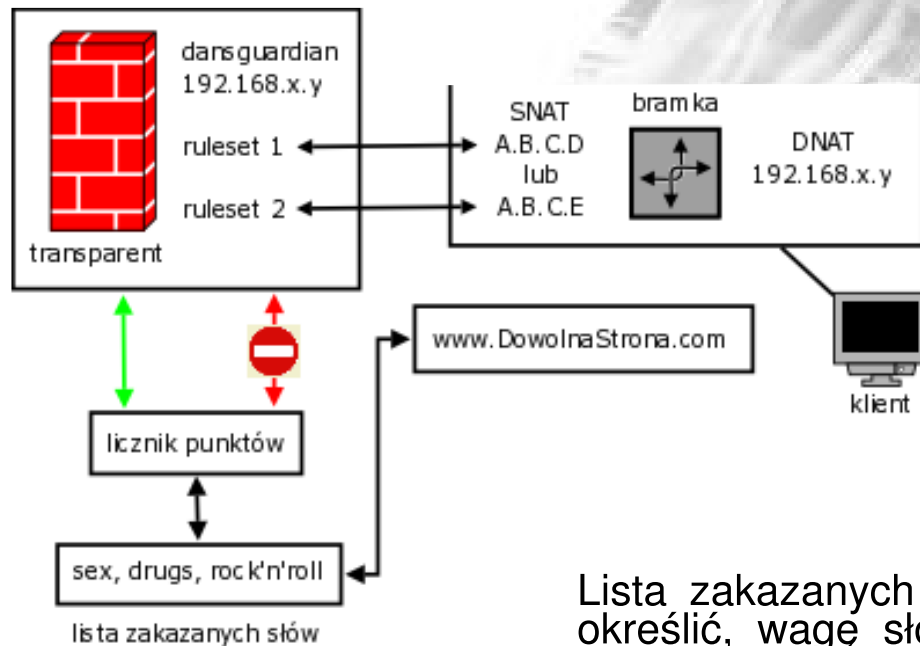


Możliwość wykonywania zapytań o odwrotny DNS, gdy użytkownik poda adres IP zamiast nazwy domenowej.

Kontrola dostępu w środowiskach heterogenicznych



- 5. Autoryzacja
- 5.3 Rodzaje filtrów
- 5.3.3 Słowa kluczowe



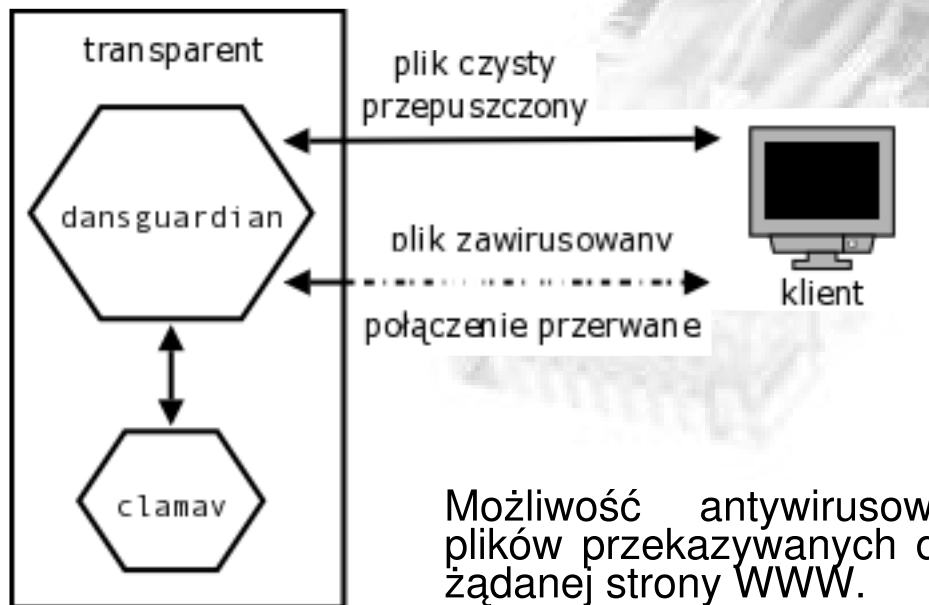
Lista zakazanych słów i licznik punktów pozwalają określić, wagę słów i ilość punktów niezbędną do zablokowania dostępu.

Kontrola dostępu w środowiskach heterogenicznych



5. Autoryzacja

5.4 Kontrola antywirusowa



Możliwość antywirusowego kontrolowania wszystkich plików przekazywanych do klienta - wszystkich składników żądanej strony WWW.

Kontrola dostępu w środowiskach heterogenicznych



5. Autoryzacja

5.5 Przekazanie bądź nie

Dostęp zezwolony, gdy spełnione są wszystkie poniższe warunki:

- URL nie jest na liście zablokowanych adresów
- podany adres nie jest adresem IP a jeśli jest, to rozwiązany revDNS nie jest zablokowanym URLeM
- strona nie zawiera nielegalnych słów lub ilość punktów za nielegalne słowa, które zawiera, jest mniejsza od limitu

Dostęp do pojedynczego pliku (nie całej strony) zabroniony, gdy:

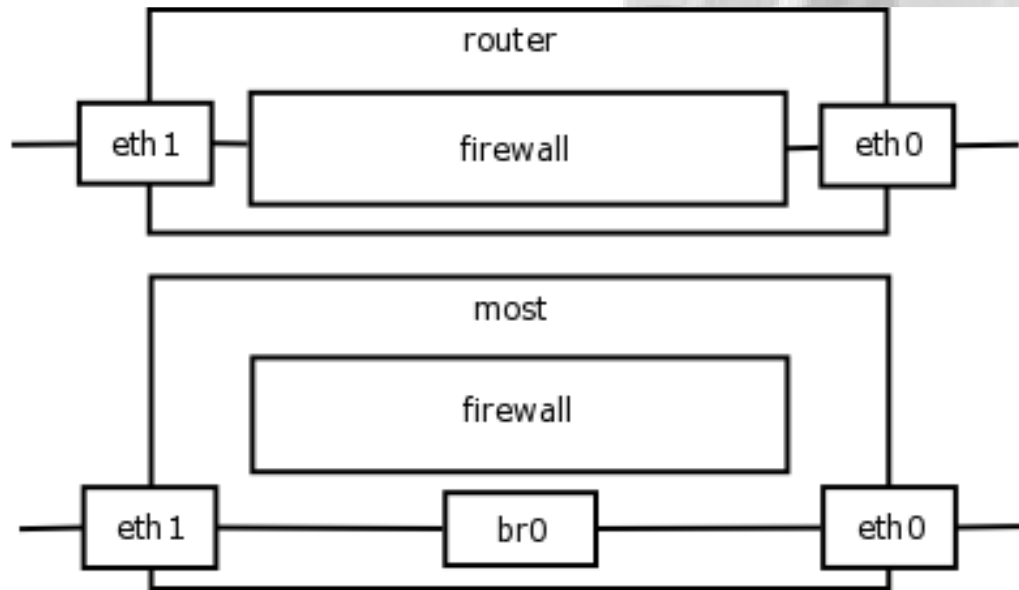
- plik pochodzi z zablokowanego URLa
- skaner antywirusowy wykazał, że plik jest zainfekowany

Kontrola dostępu w środowiskach heterogenicznych



5. Autoryzacja

5.6 Firewall

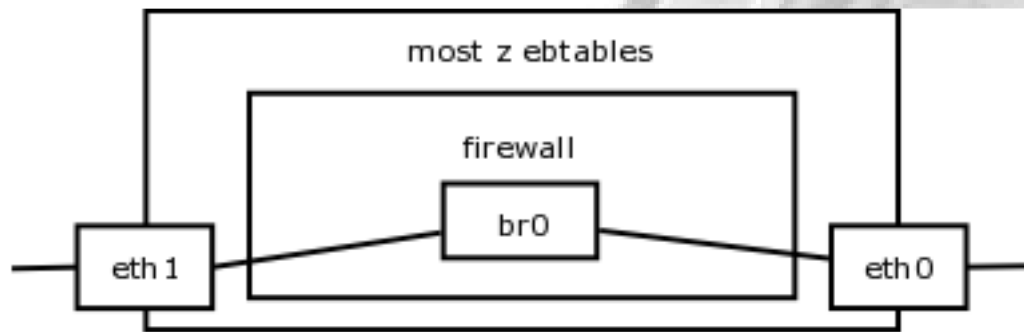


Na moście możemy również zaimplementować firewall. Jednak standardowy iptables to za mało; aby przechwycić pakiety brigeowane, potrzebujemy czegoś więcej.

Kontrola dostępu w środowiskach heterogenicznych



- 5. Autoryzacja
- 5.6 Firewall (c.d.)



EBTables to łała pozwalająca IPtables "widzieć" bridgeowane pakiety warstwy łączy danych.

Kontrola dostępu w środowiskach heterogenicznych



5. Autoryzacja 5.7 Kierowanie pakietów

Dzięki EBtables każdy pakiet przechodzący przez most może być filtrowany tak, jakbyśmy mieli do czynienia z firewallem na routerze.

Możemy na przykład w łańcuchu FORWARD zablokować ruch p2p lub połączenia do "obcych" serwerów SMTP realizowane przez maszyny inne, niż nasz serwer SMTP.

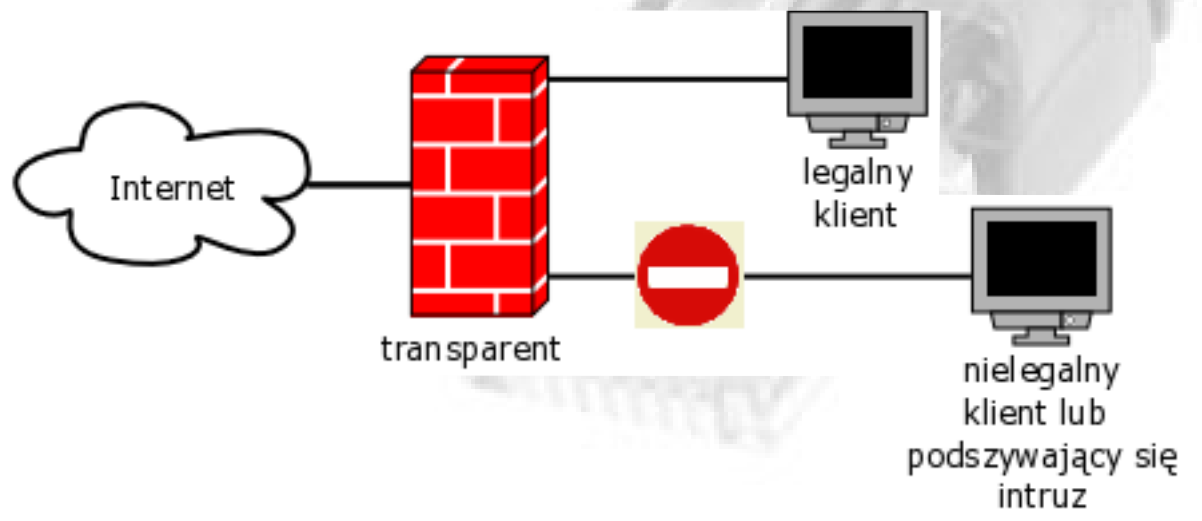
Możemy też kontrolować, czy klienci posługują się swoimi adresami IP i w ten sposób ograniczyć możliwość podszywania się.

Dzięki odpowiednim regułkom SNAT w firewallu na routerze możemy kontrolować, jaki klient gdzie ma mieć dostęp.

Kontrola dostępu w środowiskach heterogenicznych



5. Autoryzacja 5.7 Kierowanie pakietów (c.d.)



Na naszym moście możemy stworzyć centralny firewall - np. kontrolujący, czy klienci posługują się swoimi adresami IP:

```
ebtables -A FORWARD -p IPv4 --ip-src 172.16.1.4 -s ! 00:11:22:33:44:55 -j DROP
```

Kontrola dostępu w środowiskach heterogenicznych



- 5. Autoryzacja
- 5.8 Zmiana polityki

kontrolowanie polityki stacji roboczych

polityka restrykcyjna
 polityka nierestrykcyjna

Podmiot akcji

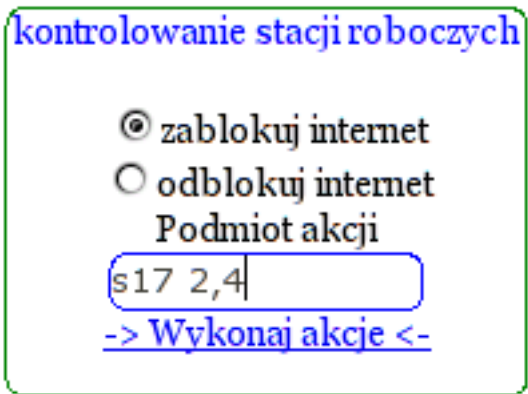
[-> Wykonaj akcje <-](#)

Za pomocą prostej aplikacji CGI możemy zmieniać politykę dla danych stacji roboczych (w przykładzie ze screena dla stacji roboczych 1,3,5 z pracowni numer 16).

Kontrola dostępu w środowiskach heterogenicznych



5. Autoryzacja 5.9 Blokowanie stacji




Za pomocą tej samej aplikacji niesfornym użytkownikom możemy zupełnie zablokować dostęp do internetu.

Kontrola dostępu w środowiskach heterogenicznych



- 5. Autoryzacja
- 5.9 Blokowanie stacji (c.d.)



Dostęp do internetu zablokowany.

To nie jest błąd komputera ani sieci.

Dostęp do internetu z tej stacji roboczej został zablokowany przez opiekuna pracowni komputerowej.

Zablokowany klient otrzymuje w przeglądarce prosty i czytelny komunikat.

Kontrola dostępu w środowiskach heterogenicznych



5. Autoryzacja

5.10 Omijanie kontroli dostępu

omijanie filtrowania

url:

[wygenerowany url](#)

-> Wykonaj akcje <-

Również za pomocą tej aplikacji możemy omijać filtrowanie DansGuardiana. Wygenerowany URL zawiera odpowiedni token, który mówi filtrującemu proxy, aby przepuścić dany URL bez sprawdzania.

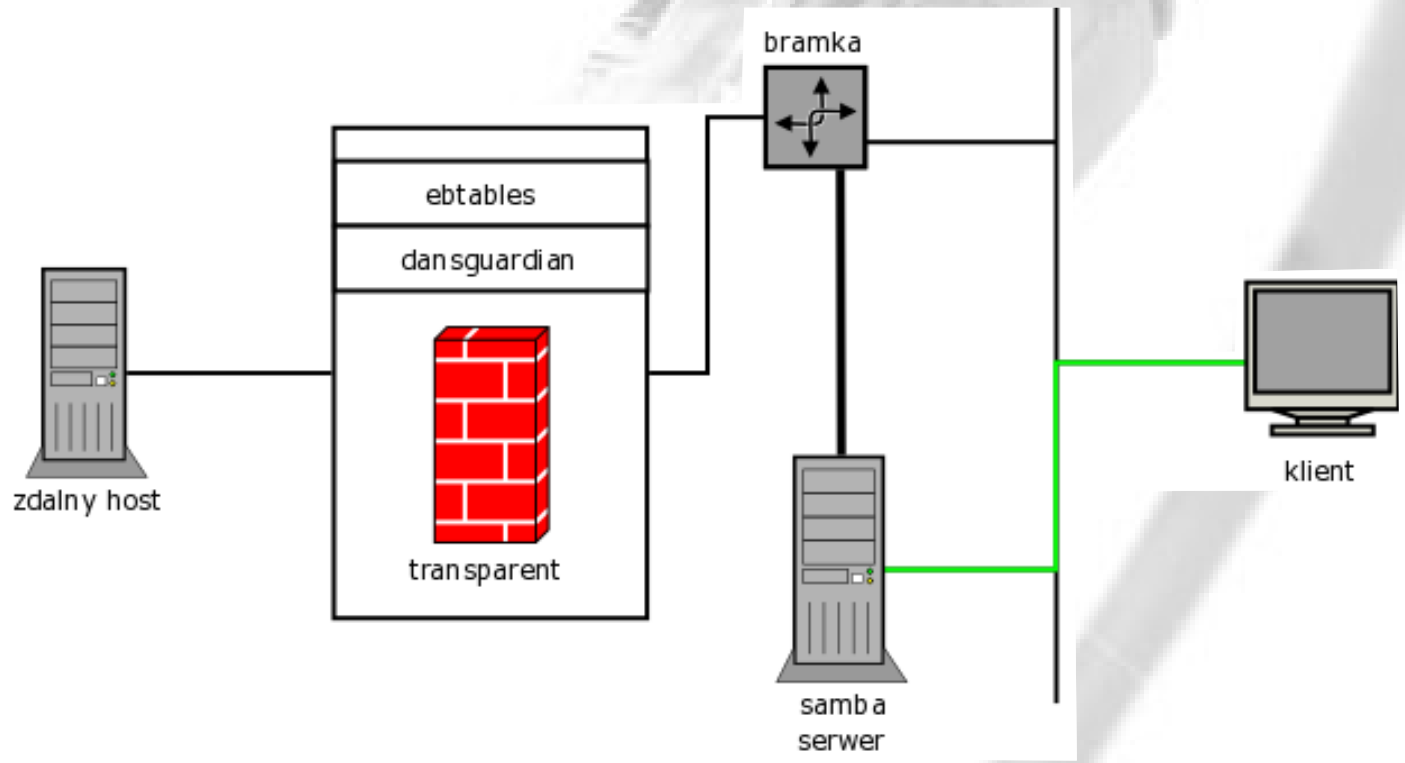
Wygenerowany URL wygląda tak:

`http://www.mw.org.pl/?GBYPASS=0F90C6F83B868BAFF168B501F997372D1206905196`

Kontrola dostępu w środowiskach heterogenicznych



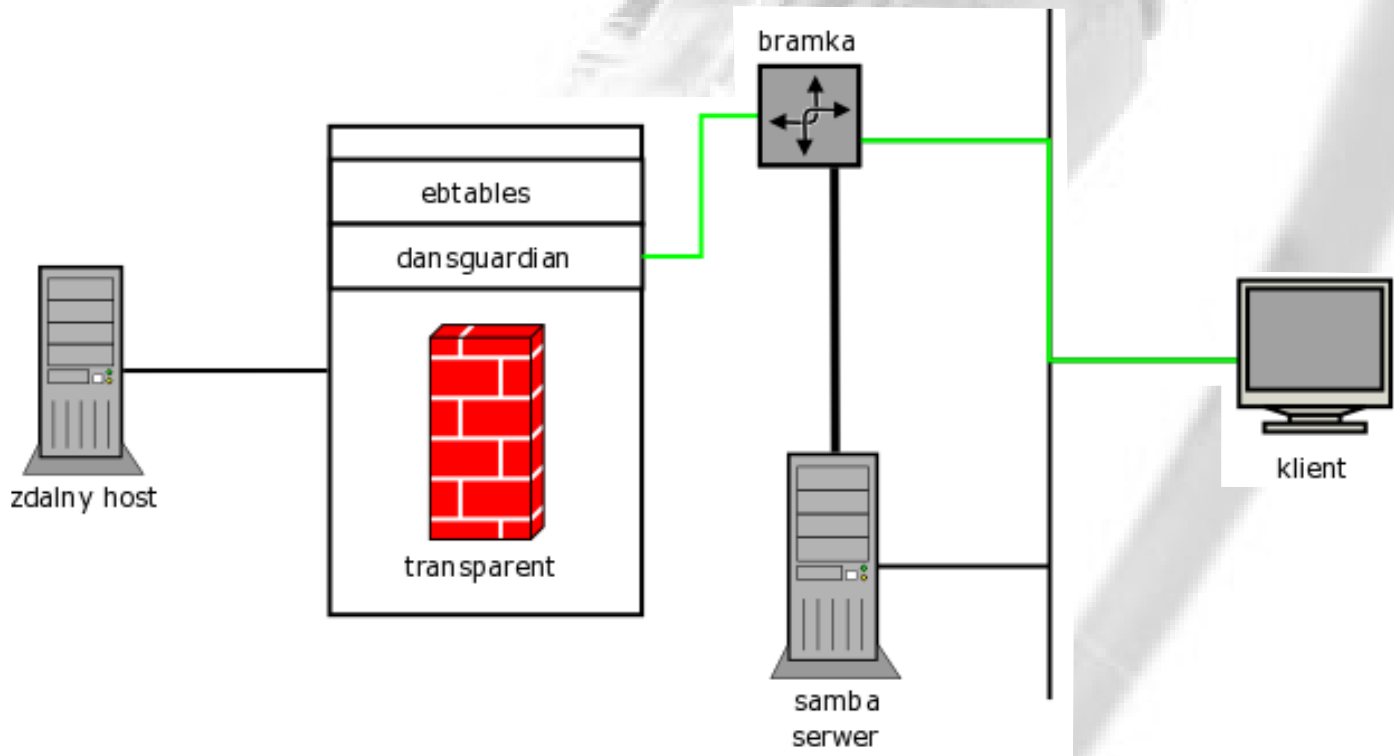
6. Przebieg połączenia 6.1 Etap 1



Kontrola dostępu w środowiskach heterogenicznych



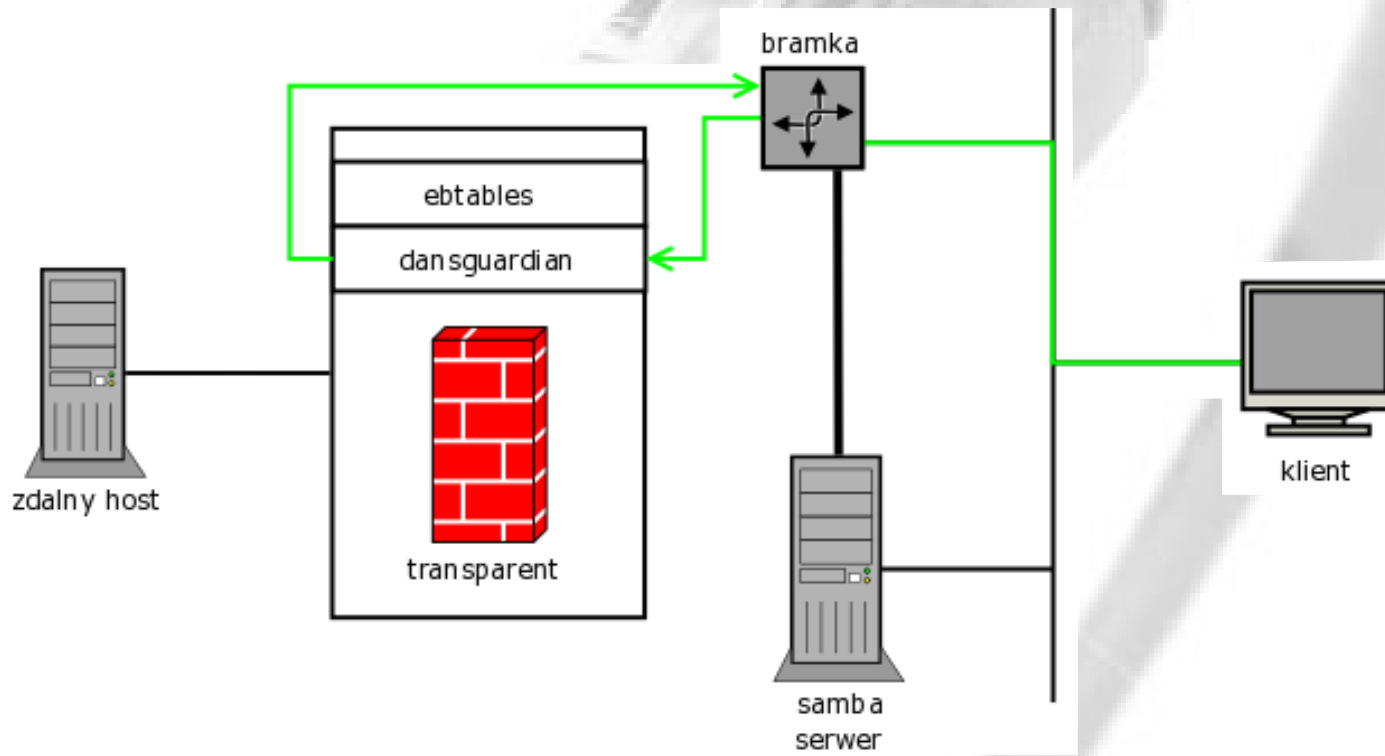
6. Przebieg połączenia 6.2 Etap 2



Kontrola dostępu w środowiskach heterogenicznych



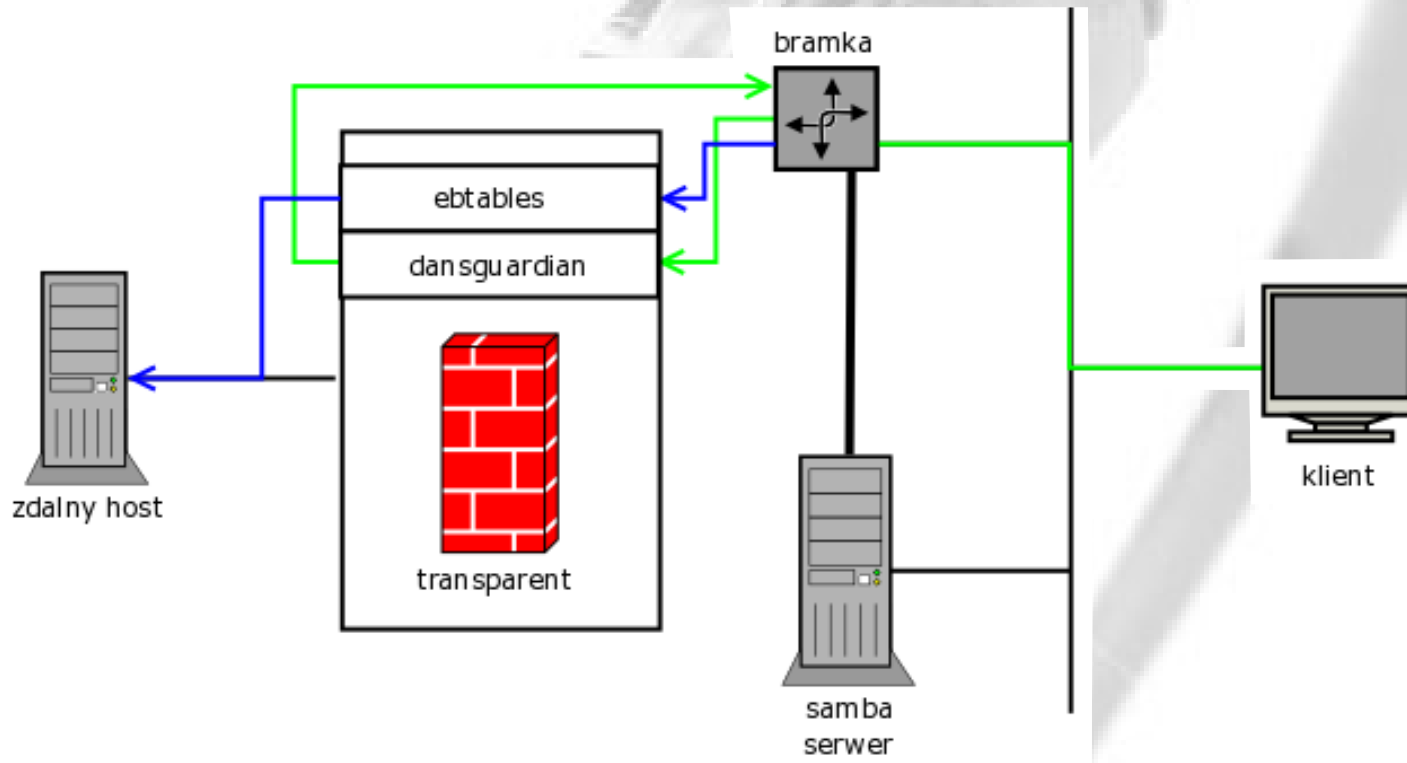
6. Przebieg połączenia 6.3 Etap 3



Kontrola dostępu w środowiskach heterogenicznych



6. Przebieg połączenia 6.4 Etap 4



Kontrola dostępu w środowiskach heterogenicznych



- 7. Uwagi
- 7.1 Wylogowywanie



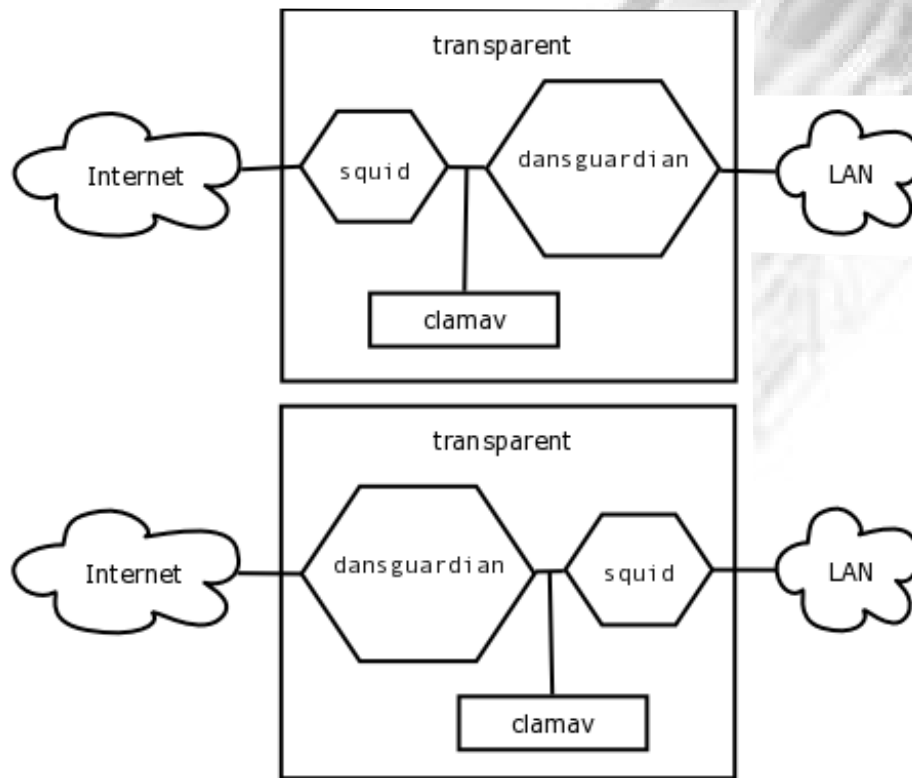
Czyszczenie reguł firewalla związanych z polityką nie jest wymagane przy wylogowywaniu użytkownika.

Kontrola dostępu w środowiskach heterogenicznych



7. Uwagi

7.2 Umieszczenie serwerów proxy



Od umiejscowienia serwerów proxy w obrębie mostu zależy to, jaki rodzaj kontroli uzyskamy.

Kontrola dostępu w środowiskach heterogenicznych



7. Uwagi

7.3 Połączenia fizyczne

- Aby uniemożliwić ominięcie kontroli mostu nad połączeniami, musimy nasz router brzegowy podłączyć bezpośrednio do sieciówki mostu.
- Serwer samby powinien być dostępny bez pośrednictwa routera, aby znał prawdziwe, niemaskowane adresy IP klientów.
- Dobrze jest mieć zestawiony bezpośredni link pomiędzy serwerem a routerem, aby przyspieszyć i uniezawodnić wymianę informacji o polityce.

Kontrola dostępu w środowiskach heterogenicznych



8. Działający przykład



Działający przykład - kontrola dostępu do zasobów internetu w pracowni komputerowej Zespołu Szkół Nr 1 z poziomu nauczyciela.

Kontrola dostępu w środowiskach heterogenicznych



9. Czas na pytania



Proszę o pytania.



Kontrola dostępu w środowiskach heterogenicznych



10. Zakończenie



Bibliografia:

- <http://www.google.pl> - pod hasłami: "ebtables", "squid", "dansguardian", "transparent proxy", "logon script", "root preexec" i podobnymi;
- "Kałamarnica na mostku" - Linux Magazine;

Kontrola dostępu w środowiskach heterogenicznych



Dziękuję za uwagę.