Firewalle, maskarady, proxy

Patryk Czarnik

Bezpieczeństwo sieci komputerowych – MSUI 2010/11

Kontrola dostępu

Polityka kontroli dostępu określa sposób dostępu do poszczególnych zasobów organizacji. Może być zależna od:

- **kierunku** – czy żądanie (dane) pochodzi z sieci wewnętrznej czy zewnętrznej,
- **usługi** – rodzaju usługi sieciowej (np. HTTP, poczta, FTP),
- **węzła sieci** – grupa adresów sieciowych, z których dostęp jest dozwolony/zabroniony,
- **użytkownika** – czasem granularność zapewniana przez adresy węzłów nie jest wystarczająca,
- **czasu** – dostęp może być dozwolony tylko w pewnych godzinach,
- **jakości usługi** – można nałożyć ograniczenia na ilość zasobów (przepustowość sieci, liczba połączeń) dostępnych dla żądającego.

Kontrola dostępu – najważniejsze wytyczne

- Organizacja powinna mieć spisaną politykę dostępu do sieci, zatwierdzoną przez „szefów”.
- Jeśli coś nie musi być dostępne – nie jest.
- Reguły zezwalające są tak ścisłe jak to możliwe.
- Wybór oprogramowania pozwalającego zrealizować politykę bezpieczeństwa (m.in. decyzja czy firewall, czy proxy zależna od ustalonej polityki).

Zapora sieciowa

Terminologia

- *Firewall*
- Tłumaczenia: ściana/zapora ogniowa/przeciwogniowa
- Może lepiej: zapora sieciowa

Funkcjonalność

- System (lub grupa systemów) wymuszający politykę kontroli dostępu
- W praktyce chodzi o filtrowanie ruchu sieciowego w oparciu o mniej lub bardziej wyrafinowane reguły
- Ochrona przed większością ataków aktywnych – pod warunkiem, właściwej konfiguracji

Umiejscowienie zapór sieciowych (1)

Granica podsieci (bramka)

- Rozwiązanie tradycyjne
- Zapewnia kontrolę administratora nad ruchem z/do całej podsieci
- Cała konfiguracja w jednym miejscu – to zaleta
- To także wada – konfiguracja specyficzna ze względu na maszyny wewnątrz sieci może bardzo sie rozrosnąć, a jej aktualizacja może być uciążliwa
- Nie uwzględnia ruchu wewnątrz sieci

Umiejscowienie zapór sieciowych (2)

Idywidualny komputer (np. terminal użytkownia)

- Rozwiązanie zalecane od niedawna
- Jako dodatek do poprzedniego, a nie zamiast
- A gdy komputer nie jest chroniony zaporą w bramce, to indywidualna zapora zalecana tym bardziej :)
- Łatwiejsza konfiguracja specyficzna dla danej maszyny (np. uwzględniająca mające tam działać aplikacje)
- Możliwa konfiguracja specyficzna dla użytkowników (o ile oprogramowanie pozwala)

Rodzaje zapór sieciowych

- Statyczne (bezstanowe, pakietowe) – „pierwsza generacja”.
- Stanowe (dynamiczne) – „druga generacja”.
- Poziomu aplikacji (oparte o proxy) – „ trzecia generacja”.
- Możliwe dodatkowe funkcjonalności (często połączone we wspólną infrastrukturę):
  - translacja adresów (NAT),
  - maskarada,
  - dodatkowe funkcje proxy.

Skąd wiemy czy wpuścić?

Podstawowa metoda różnicowania żądań – informacje zawarte w nagłówkach pakietów, m.in.:

- port (uznajemy za rodzaj usługi); 20000 zarezerwowanych i standardowo używanych portów, np.:
  - 23 – Telnet,
  - 25 – SMTP,
  - 53 – DNS,
  - 110 – POP-3,
- adres źródłowy żądania,
- adres docelowy żądania.

Statyczne filtrowanie pakietów

- Każdy pakiet traktowany indywidualnie.
- Dopuszcza lub blokuje połączenia pomiędzy określonymi parami portów.
- Najsłabszy sposób kontroli dostępu:
  - nie bierze pod uwagę dynamiki i historii ruchu sieciowego.
- Wiele routerów ma wbudowaną możliwość statycznego filtrowania pakietów.

Dynamiczne filtrowanie pakietów

- Tablica połączeń, możliwość pamiętania stanu połączenia.
- Dopasowywanie pakietu do połączenia w tablicy (lub nowy wpis).
- Bardziej dokładna kontrola ruchu, np.:
  - możliwość odrzucania pakietów wyrwanych z kontekstu,
  - możliwość akceptacji pakietów wychodzących należących do zaakceptowanego wcześniej połączenia przychodzącego (i tylko takich).
- `iptables` – reguły bezstanowe i stanowe, wtyczki dla poziomu aplikacji

Serwery pośredniczące (Proxy)

- Aplikacja służąca jako pośrednik w ruchu pomiędzy siecią wewnętrzną a Internetem.
- Dzięki temu węzły sieci wewnętrznej nie są nigdy bezpośrednio podłączone do komputerów w Internecie.
- Mogą uzupełniać filtrowanie pakietów przez zapory.
- Działają na poziomie aplikacji (np. HTTP lub FTP), a więc mają dostęp nie tylko do nagłówków pakietu ale także do danych w nich zawartych.
- Dlatego możemy za ich pomocą wymusić kontrolę dostępu na wyższym poziomie szczegółowości niż w przypadku standardowych zapór.

Application Proxy Firewall

- Zapora rozumie poziom aplikacji i jest w stanie kontrolować ruch w zależności od jego znaczenia na poziomie aplikacji.
- Filtrowanie na poziomie aplikacji; przykładowe zastosowania:
  - FTP – blokowanie wszystkich żądań PUT oraz MPUT.
  - HTTP – dostęp do określonych katalogów tylko dla określonych adresów źródłowych.
- Możliwość odszyfrowywania danych i analizowania treści – o ile skonfigurowane parametry kryptograficzne (np. znany prywatny klucz SSL serwera https).
- Uwierzytelnianie użytkowników nawiązujących połączenia.
- Zapamiętywanie informacji o połączeniach do późniejszej analizy.
- Funkcjonalność odpowiada funkcjonalności serwerów proxy, ale tu jest przezroczysta dla aplikacji.

Wady i koszty serwerów proxy

- Niezbędna osobna implementacja dla każdego nowego protokołu/usługi.
- Nie przezroczyste – klient musi skonfigurować aplikację tak aby korzystała ona z serwera pośredniczącego.
  - Nie dotyczy to zapór typu proxy, tylko zwykłych serwerów proxy.
- Bardziej skomplikowana niż w przypadku prostych zapór konfiguracja.

Przykładowa konfiguracja iptables (nieciekawa :))

```
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

SOCKS

- **Socks** – inny typ serwerów pośredniczących.
- Można go porównać do centrali telefonicznej która zajmuje się łączeniem połączeń przychodzących z wychodzącymi.
- Serwery SOCKS działają z TCP oraz UDP (od wersji 5tej).
- Zapewniają zarówno logowanie jak i silne uwierzytelniania (także od wersji 5.0) połączeń.
- SOCKS może łączyć węzły z adresami IP v.4, IP v.6 jak i pomiędzy nimi.

Działanie SOCKS

Konfiguracja obsługi SOCKS po stronie klienta:
Aby skonfigurować połączenie przez SOCKS po stronie klienta niezbędna jest biblioteka SOCKS która jest warstwą pośrednicząca pomiędzy warstwą aplikacji i warstwą gniazd. Aplikacja jest w ten sposób "oszukiwana" - wywołania funkcji z API gniazd i DNS są zastępowane przez wywołania funkcji z SOCKS Lib o tej samej nazwie. Rozwiązanie takie jest przezroczyste dla aplikacji klienckich.

Tłumaczenie adresów (Network Address Translation)

- Ukrywanie adresów wewnętrznych przed siecią zewnętrzną.
- Translacja adresu źródłowego z wewnętrznego na adres z puli zewnętrznej przy wychodzeniu pakietu na zewnątrz.
- Translacja adresu docelowego z zewnętrznego na odpowiadający mu adres wewnętrzny przy przychodzeniu pakietu z zewnątrz.
- Na poziomie IP.
- „NAT 1 do 1” – relacja 1-1 między adresami wewnętrznymi a zewnętrznymi.

Zalety i wady NAT

- Zalety:
  - Serwery NAT są dostępne dla większości systemów operacyjnych (w Linuxie zintegrowane z firewallami).
  - NAT nie wymaga specjalnego oprogramowania na poziomie aplikacji.
  - NAT jest w wysokim stopniu konfigurowalne.
- Wady:
  - Konieczność zapewnienia dużej puli adresowej dla odpowiednio dużej sieci.

Maskarada

- Nazywana także **NAT 1 do wielu** lub PAT (*Port Address Translation*).
- Jeden adres IP (zwykle samego serwera maskarady) dla wszystkich adresów wewnętrznych.
- Rozróżnienie na poziomie portów.
- Działanie:
  1. serwer w sieci wewnętrznej wysyła pakiet do Internetu przez serwer Maskarady,
  2. serwer zmienia w pakiecie adres źródłowy na własny oraz port źródłowy na wolny zapisując jednocześnie pary adresów i portów w specjalnej tablicy,
  3. gdy nadejdzie odpowiedź z Internetu serwer Maskarady sprawdza czy ma odpowiednią parę adresów i portów w tablicy i jeśli tak to tłumaczy adres i port na ich odpowiedniki wzięte z tablicy i wysyła tak zmieniony pakiet do sieci wewnętrznej.

Zalety i wady maskarady

- Zalety:
  - potrzebny jest tylko jeden adres IP
  - nie wymaga specjalnego wsparcia ze strony aplikacji
  - dobrze zintegrowane z oprogramowaniem zapór sieciowych - zapewnia większe bezpieczeństwo
- Wady:
  - mniejsze wsparcie (ale w Linuxie jest OK)
  - pewne typy protokołów wymagają specjalnego wsparcia ze strony zapory aby działać poprawnie (dostępne na Linuksie),
  - serwery w sieci wewnętrznej nie będą widoczne dla klientów z zewnątrz - każdy ruch wchodzący musi być wcześniej zainicjowany przez węzeł w sieci wewnętrznej,

IDS – Intrusion Detection Systems

Systemy IDS są dopełnieniem zapór sieciowych. Ich zadaniem jest monitorowanie sieci i wykrywanie wszelkich podejrzanych zachowań. Jeśli założymy, że włamywacz prześliznął się przez zaporę to czeka na niego system IDS, który będzie logował wszelką aktywność sieciową i ewentualnie podniesie alarm (np. przez wysłanie listu do administratora systemu).
Systemy IDS korzystają z bazy danych zawierającej historię dotychczasowego ruchu w sieci i dokonują na jej podstawie analizy statystycznej która pozwala im odróżniać zachowania typowe od nietypowych. Potrafią też rozpoznawać typowe ataki na podstawie wbudowanych w nie algorytmów.
Zaletą systemów typu IDS jest też to, że utrudniają ataki nadchodzące z wnętrza systemu (sieci wewnętrznej).

Odmowa świadczenia usług — (Denial of Services)

Jest to atak aktywny którego celem nie jest włamanie się do systemu, ale uniemożliwienie mu normalnej pracy. Zazwyczaj polega na zapchaniu serwerów lawiną pakietów.
Jeśli będzie to atak rozproszony to przy obecnej infrastrukturze Internetu jest on właściwie nie do uniknięcia. Możemy jedynie starać się odciąć fizycznie ruch przychodzący od podejrzanych węzłów kontaktując się z administratorami routerów leżących na jego trasie.