Firewalle i SNMP

Krzysztof Ciebiera

10 czerwca 2006

Kontrola dostępu

Kontrola dostępu Polityka kontroli dostępu określa sposób dostępu do poszczególnych zasobów (przepustowości sieci, pamięci dyskowej, zasobów obliczeniowych itp.) organizacji. Polityka kontroli dostępu może być zależna od:

- Kierunku - czy żądanie (dane) pochodzi z sieci wewnętrznej czy zewnętrznej
- Usługi - rodzaju usługi sieciowej (np. WWW - HTTP, poczta - SMTP, przesyłanie danych - FTP)
- Węzła sieci - można określić grupę adresów sieciowych z których dostęp jest dozwolony/zabroniony
- Użytkownika - czasem granularność zapewniana przez adresy węzłów nie jest wystarczająca
- Czasu - w pewnych godzinach dostęp może być dozwolony
- Jakości usługi - można nałożyć ograniczenia na ilość zasobów (np. przepustowość sieci) dostępnych dla żądającego

Ściana ogniowa

Ściana ogniowa to system (lub grupa systemów) wymuszająca politykę kontroli dostępu.
Zazwyczaj kontrola dostępu odbywa się pomiędzy siecią wewnętrzną, a Internetem. Możliwe są jednak także inne zastosowania.
Ściany ogniowe mogą służyć do ochrony przed większością ataków aktywnych - pod warunkiem, że zostały właściwie skonfigurowane.
Podstawowa reguła przy ustalaniu polityki dostępu brzmi:
Jeśli usługa nie musi być dostępna to należy ją zablokować.

Skąd wiemy kto ma dostęp do usługi?

Podstawową metodą różnicowania żądań dostępu do systemu jest wykorzystanie informacji zawartej w nagłówkach pakietów zawierających żądanie.
Port docelowy - wskazuje na typ usługi do której odnosi się żądanie np.

- 23 - Telnet
- 25 - SMTP
- 53 - DNS
- 110 - POP-3

Istnieje 20000 zarezerwowanych i powszechnie znanych portów.

Statyczne filtrowanie pakietów

Statyczne filtrowanie pakietów na podstawie informacji zawartej w nagłówku pakietu dopuszcza lub blokuje połączenia pomiędzy określonymi parami portów.
Jest to najsłabszy sposób kontroli dostępu jako, że nie bierze pod uwagę dynamiki i historii ruchu sieciowego.
Wiele ruterów ma wbudowaną możliwość statycznego filtrowania pakietów.

Dynamiczne filtrowanie pakietów

Dynamiczne filtrowanie korzysta z tablicy połączeń w celu monitorowania stanu komunikacji. Ta cecha pozwala na dokładniejsze "przykrawanieżuchu sieciowego.
Jeśli ktoś zaatakuje system wysyłając pakiet podszywa się pod dozwolony węzeł sieci ale z zawartością mogącą spowodować zapaść systemu (np. przez przepełnienie stosu) to ściana ogniowa ze statycznym filtrowaniem przepuści taki pakiet.
Jeśli jednak skorzystamy z filtrowania dynamicznego to ściana ogniowa na podstawie tablicy połączeń uzna, że pakiet przychodzący nie należy do żadnego aktywnego połączenia i odrzuci go.

Serwery pośredniczące (Proxy)

Serwery pośredniczące to aplikacje służącej jako pośrednik w ruchu pomiędzy siecią wewnętrzną, a Internetem. Dzięki temu węzły sieci wewnętrznej nie są nigdy bezpośrednio podłączone do komputerów w Internecie.
Serwery takie mogą uzupełniać filtrowanie pakietów przez ściany ogniowe. Serwery pośredniczące działa ją na poziomie aplikacji (np. HTTP lub FTP), a więc ma ją 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 ścian ogniowych. Na przykład Proxy dla FTP może blokować wszystkie żądania PUT oraz MPUT.

Serwery pośredniczące (Proxy) cd.

Oprócz filtrowania serwery Proxy mogą spełniać dodatkowe funkcje:

- uwierzytelniać użytkowników nawiązujących połączenia
- zapamiętywać informacje o połączeniach do późniejszej analizy
- służyć jako cache (np. serwer Proxy dla HTTP)

Do wad serwerów pośredniczących należą:

- niezbędna jest osobna implementacja dla każdego nowego protokołu/usługi.
- nie są przeźroczyste - klient musi skonfigurować aplikację tak aby korzystała ona z serwera pośredniczącego
- bardziej skomplikowana niż w przypadku ścian ogniowych konfiguracja

Socks

Innym typem serwerów pośredniczących jest Socks. Można go porównać do centrali telefonicznej która zajmuje się łączeniem połączeń przychodzących z wychodzącymi.
Serwery SOCKS działa ją z TCP oraz UDP (od wersji 5tej) oraz zapewnia ją 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.
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 ószukiwana- wywołania funkcji z API gniazd i DNS są zastępowane przez wywołania funkcji z SOCKS Lib o tej samej nazwie. Rozwiązanie takie jest przeźroczyste dla aplikacji klienckich.

Tłumaczenie adresów (Network Address Translation)

Jedną z metod chronienia informacji o własnej sieci jest ukrywanie adresów komputerów do niej należących. Zadaniem tym zajmuje się specjalny serwer służący jako tłumacz na styku sieci wewnętrznej i Internetu. Tłumacz taki ma pulę zarejestrowanych adresów Internetowych z której mogą korzystać węzły sieci wewnętrznej jeśli chcą dokonać połączenia z Internetem. Zadaniem tłumacza jest utrzymywanie tablicy powiązań pomiędzy komputerami w sieci wewnętrznej, a adresami z puli oraz tłumaczenie odpowiednio adresu źródła (w pakietach wychodzących) oraz przeznaczenia w pakietach wchodzących do sieci wewnętrznej.

Tłumaczenie adresów (Network Address Translation) cd.

Zalety korzystania z NAT (Network Address Translation):

- serwery NAT są dostępne dla większości systemów operacyjnych
- NAT nie wymaga specjalnego oprogramowania na poziomie aplikacji
- NAT jest w wysokim stopniu konfigurowalne

Główną wada systemów NAT jest konieczność zapewnienia dużej puli adresowej dla odpowiednio dużej sieci - co może być dość kosztowne.

Maskarada

Nazywana także ŃAT 1 do wielu". Serwer Maskarady zamiast tłumaczyć adresy węzłów w sieci wewnętrznej na adresy z puli użycza im swojego własnego adresu IP.
Jak to działa?

- serwer w sieci wewnętrznej wysyła pakiet do Internetu przez serwer Maskarady
- serwer zmienia w pakiecie adres źródłowy na własny oraz port źródłowy na wolny zapisując jednocześnie pary adresów i portów w specjalnej tablicy
- 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

Maskarada cd.

Zalety Maskarady:

- potrzebny jest tylko jeden adres IP
- nie wymaga specjalnego wsparcia ze strony aplikacji
- dobrze zintegrowane z oprogramowaniem ścian ogniowych - zapewnia większe bezpieczeństwo

Wady:

- pewne typy protokołów wymaga ją specjalnego wsparcia ze strony ściany ogniowej 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 ścian ogniowych. Ich zadaniem jest monitorowanie sieci i wykrywanie wszelkich podejrzanych zachowań. Jeśli założymy, że włamywacz prześliznął się przez ścianę ogniową 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 korzysta ją 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 utrudnia ją 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 ruterów leżących na jego trasie.

Elementy architektury zarządzanie siecią w SNMP

- stacja zarządzająca
- agent zarządzający
- baza informacji
- protokół zarządzania siecią

Stacja zarządzająca powinna być wyposażona w następujące elementy:

- zestaw aplikacji służących do analizy informacji, naprawiania błędów itp.
- interfejs służący administratorowi do obserwacji i kontroli sieci
- możliwość przekładania wymagań administratora sieci na faktyczną możliwość obserwacji i kontroli elementów sieci
- bazę danych zawierającą informacje z baz informacji administracyjnych (MIB) wszystkich jednostek w administrowanej sieci

Polecenia SNMP

- GetRequest - dla każdego obiektu wymienionego w poleceniu zwróć wartość tego obiektu
- GetNextRequest - dla każdego obiektu wymienionego w poleceniu zwróć wartość następnego obiektu (w porządku leksykograficznym danego MIBa)
- GetBulk (SNMPv2) - dla każdego obiektu wymienionego w poleceniu zwróć wartość następnych N obiektów
- SetRequest - dla każdego obiektu wymienionego w poleceniu ustaw wartość na wymienioną w poleceniu
- Trap - prześlij informację o zaistniałym zdarzeniu (agent do menedżera)
- Inform (SNMPv2) - prześlij informację o zaistniałym zdarzeniu (menedżer do menedżera)
- GetResponse - odpowiedz na żądanie menedżera

Elementy bezpieczeństwa w SNMP

- Uwierzytelnianie (SNMPv2) - procedura umożliwiająca stronie odbierającej sprawdzenie, że komunikat pochodzi z danego źródła i ma właściwy czas. Realizuje się ją przez dołączenie do komunikatu dodatkowej informacji.
- Prywatność (SNMPv2) - ochrona danych przed odczytaniem przez nieupoważnionych odbiorców. Realizuje się ją przez szyfrowanie danych.
- Kontrola dostępu - ograniczenie dostępu menedżera do konkretnego fragmentu MIBa oraz określonego zbioru poleceń.

Społeczności w SNMPv1

Każdy agent w systemie dysponuje swoją własną MIB i ma możliwość kontrolowania dostępu do niej przez wielu menedżerów. Kontrola ta ma następujące aspekty:

- usługa uwierzytelniania - agent może zastrzec prawo dostępu do MIB tylko dla pewnych menedżerów
- ograniczenia dostępu - agent może przydzielać różnych przywilejów różnym menedżerom
- usługa pełnomocnictwa - agent może działać jako pośrednik innych agentów. Wymaga to implementacji poprzednich dwóch usług dla agentów względem których pełniona jest funkcja pośrednika

W celu realizacji wszystkich tych aspektów definiuje się społeczność SNMP.

Społeczności w SNMPv1 cd.

Społeczność to relacje łączące agenta i zbiór menedżerów SNMP w ramach których procedury kontrolne mają określone cechy. Społeczność ma charakter lokalny zdefiniowany u agenta. Agent tworzy społeczność dla żądanej kombinacji cech:

- uwierzytelniania
- kontroli dostępu
- pełnomocnictwa

Każdej społeczności nadaje się unikalną (w ramach agenta) nazwę którą należący do niej agenci muszą podawać przy wszystkich operacjach związanych z danym agentem.
Agent może ustanowić wiele społeczności. Menedżerowie mogą należeć do wielu społeczności.

Polityka ograniczeń dostępu w SNMPv1 Każdej społeczności SNMP odpowiada profil społeczności określający polityk,e dostępu do obiektów MIB. Profil taki ma dwa aspekty:

- widok MIB - to zbiór obiektów MIB do których dostęp ma dana społeczność
- tryb dostępu - określa polecenia które możliwe są do wykonania na danym obiekcie. Tryb dostępu w SNMPv1 to następujący zbiór: $\{READ - ONLY, READ - WRITE\}$

Bezpieczeństwo w SNMPv2

Środki zapewniania bezpieczeństwa w SNMPv2 służą do ochrony przed następującymi zagrożeniami:

- ujawnianie - przeciwnik może śledzić informacje wymieniane przez menedżera i agenta i w ten sposób poznać wartość zarządzanych obiektów oraz uzyskać informacje o wydarzeniach
- maskarada - przeciwnik może starać się podszyć pod członka społeczności w celu wykonania niedozwolonej dla siebie operacji
- modyfikacja treści komunikatu - przeciwnik może zmienić wygenerowany przez członka społeczności komunikat w trakcie przesyłania w taki sposób aby doprowadzić do wykonania niedozwolonej operacji zarządzania.
- modyfikacja kolejności i czasu komunikatów w celu doprowadzenia do wykonania niedozwolonych operacji przeciwnik może zmieniać kolejność, opóźniać lub powtarzać komunikaty SNMP

Bezpieczeństwo w SNMPv2 cd.

SNMPv2 nie chroni natomiast przed następującymi zagrożeniami:

- uniemożliwienie działania - przeciwnik może zablokować wymianę informacji między agentem a menedżerem
- analiza ruchu - przeciwnik może śledzić schemat ruchu pomiędzy menedżerem i agentami

Strony w SNMPv2

Komunikaty SNMPv2 zawierają informacje o tożsamości źródła i miejsca przeznaczenia. Każda jednostka może jednak zachowywać się inaczej pod względem bezpieczeństwa w zależności nie tylko od tożsamości drugiej strony ale także od właśnie obsługiwanego programu. Rola jednostki w SNMPv2 zależy więc od kontekstu jej działania. Ideę roli wyraża pojęcie strony. Jednostki mogą obejmować wiele stron.
Każda jednostka SNMPv2 dysponuje bazą danych o zawierającą informacje o wszystkich znanych jej stronach, są to:

- Strony lokalne - zbiór stron na których działania wykonuje lokalna jednostka SNMPv2 czyli zbiór ról tej jednostki
- Strony reprezentowane - zbiór stron jednostek reprezentowanych przez daną jednostkę SNMPv2
- Strony odległe - zbiór stron, których działania realizują inne jednostki SNMPv2 z którymi dana jednostka może wchodzić w interakcje

Prywatność Dla każdej znanej jednostki SNMPv2 baza danych stron zawiera trzy zmienne których znaczenie zależy od stosowanego protokołu prywatności

- *partyPrivProtocol* - określa protokół prywatności i mechanizm ochrony komunikatów otrzymywanych przez daną stronę. Wartość noPriv oznacza, że komunikaty otrzymywane przez stronę nie są chronione przez ujawnieniem.
- *partyPrivPrivate* - tajna wartość której wymaga protokół prywatności. Może to być klucz szyfru symetrycznego lub prywatny klucz szyfru asymetrycznego.
- *partyPrivPublic* - dowolna wartość jawna potrzebna w protokole prywatności. Może to być klucz publiczny w systemie asymetrycznym.

Mechanizm zapewniania prywatności w aktualnej wersji SNMPv2 polega na szyfrowaniu z użyciem algorytmu DES i wymaga aby obie strony dzieliły wspólny klucz szyfrujący. Struktura bazy danych umożliwia jednak zastosowanie innych algorytmów szyfrujących (symetrycznych bądź asymetrycznych).

Uwierzytelnianie

Dla każdej strony znanej danej jednostce SNMPv2 baza danych stron zawiera pięć zmiennych:

- *partyAuthProtocol* - określa protokół uwierzytelniania stosowany do potwierdzania pochodzenia i nienaruszalności wysyłanych komunikatów. Wartość noAuth wskazuję, że komunikaty wysyłane przez stronę nie podlegają uwierzytelnianiu.
- *partyAuthClock* - określa aktualny czas lokalny danej strony
- *partyAuthPrivate* - tajna wartość wymagana przez protokół uwierzytelniania. Może to być tajna wartość hasha z komunikatu, klucz szyfru symetrycznego lub prywatny klucz szyfru asymetrycznego.
- *partyAuthPublic* - dowolna wartość jawna potrzebna w protokole uwierzytelniania. Może to być klucz publiczny w systemie asymetrycznym.
- *partyAuthLifetime* - narzucona administracyjnie górna granica akceptowanego opóźnienia dostarczania komunikatów generowanych przez daną stronę

Kontrola dostępu

Na politykę kontroli dostępu składają się cztery elementy:

- strona przeznaczenia - strona SNMP wykonująca operację zarządzania na żądanie strony źródłowej
- strona źródłowa - strona SNMP żądająca wykonania operacji nażądanie stron przeznaczenia
- zasoby - informacje zarządzania na których można przeprowadzać żądane operacje zarządzania w postaci lokalnego widoku MIB lub relacji pełnomocnictwa, nazywane także kontekstem
- przywileje - operacje dozwolone, zdefiniowane jako dozwolone PDU przynależące do danego kontekstu i do których wykonania w imieniu podmiotu jest uprawniony odbiorca

Kontrola dostępu cd.

Kontrolę dostępu określają informacje zawarte w MIB stron. Baza ta składa się z czterech tablic:

- tablicy stron - zawiera po jednej pozycji na każdą stronę znaną lokalnemu agentowi. Każda pozycja zawiera parametry uwierzytelniania i prywatności. Raz na sekundę lokalny menedżer musi zwiększyć wartość zegara dla każdej pozycji tablicy
- tablica kontekstów - może zawierać pozycje związane z informacjami lokalnymi oraz relacjami pełnomocnictwa
- tablica kontroli dostępu - jest indeksowana stroną źródłową, stroną przeznaczenia i kontekstem. Każda pozycja zawiera zbiór PDU akceptowanych przez odbiorcę
- tablica widoków MIB - składa się ze zbioru widoków