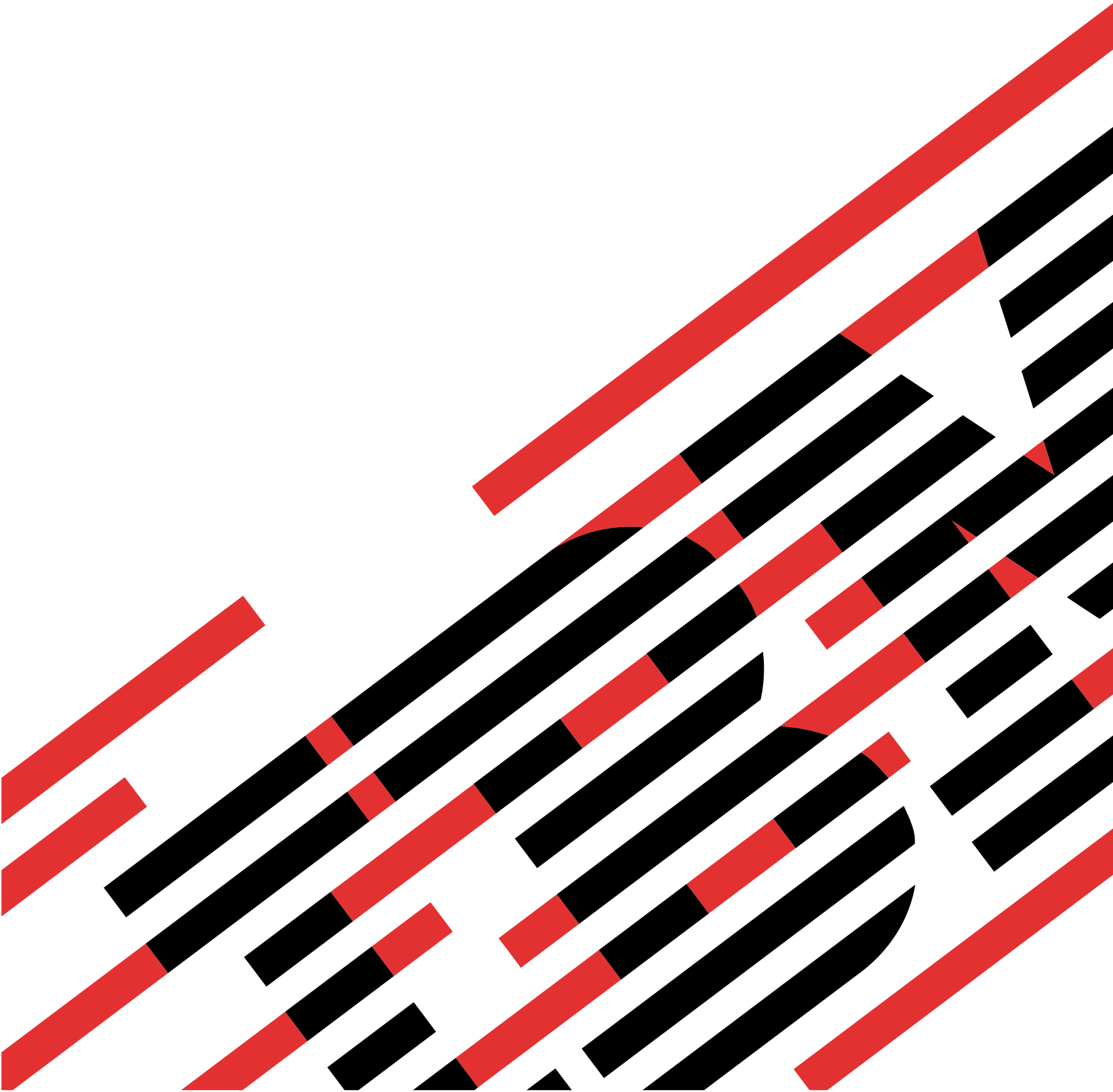
IBM

eserver

iSeries

IBM SecureWay: iSeries 400 i Internet



IBM

@server

iSeries

IBM SecureWay: iSeries 400 i Internet

Spis treści

Część 1. IBM SecureWay: iSeries i Internet

Dostęp do Internetu z sieci LAN jest ważnym krokiem w rozwoju sieci, wymagającym ponownej oceny wymagań ochrony. Na szczęście serwer iSeries 400 ma wbudowane zintegrowane rozwiązania programowe i architekturę ochrony, która pozwala budować silną obronę przed potencjalnymi zagrożeniami ze strony użytkowników Internetu. Poprawne korzystanie z propozycji ochrony systemu iSeries gwarantuje, że zarówno klienci, jak i pracownicy czy partnerzy handlowi firmy będą mogli otrzymać informacje potrzebne do współpracy w chronionym środowisku.

Przedstawione tu informacje mogą służyć jako kompendium wiedzy na temat znanych zagrożeń dla ochrony systemu oraz wpływu tych zagrożeń na przedsięwzięcia związane z Internetem i e-biznesem. Przedstawione zostaną także kryteria oceny potencjalnych niebezpieczeństw w porównaniu z korzyściami płynącymi ze stosowania różnych opcji ochrony, które są dostępne w serwerze iSeries. Wreszcie, zawarto tu praktyczne wskazówki dotyczące wdrożenia planu ochrony sieci, który będzie dopasowany do konkretnej sytuacji.

Aby dowiedzieć się więcej na temat niebezpieczeństw związanych z korzystaniem z Internetu oraz wbudowanych w serwer iSeries mechanizmów ochronnych, których można użyć do zabezpieczenia systemów i zasobów, należy przejrzeć poniżej wymienione sekcje:

- **Co nowego w wersji V5R1**
  Tu zawarto informacje na temat zmian i nowych funkcji w zakresie ochrony internetowej serwera iSeries w wersji V5R1.
- **Drukowanie tego dokumentu**
  Tu opisano procedurę odczytywania i drukowania niniejszego tekstu w formacie Adobe Acrobat.
- **iSeries a ochrona internetowa**
  Tu przedstawiono ogólne informacje na temat zalet funkcji zabezpieczających iSeries z punktu widzenia e-biznesu oraz możliwych opcji w tym zakresie.
- **Planowanie ochrony internetowej**
  Tu opisano sposób tworzenia strategii ochrony na potrzeby Internetu i e-biznesu.
- **Poziomy ochrony systemu iSeries dla podstawowego zakresu gotowości internetowej**
  Na podstawie tych informacji można ustalić, jakie elementy ochrony systemu powinny zostać wdrożone przed podłączeniem go do Internetu.
- **Ochrona na poziomie sieci**
  Tu zawarto informacje na temat zabezpieczeń na poziomie sieci, które należałoby uaktywnić w celu ochrony zasobów wewnętrznych.
- **Ochrona na poziomie aplikacji**
  Tu opisano powszechne zagrożenia związane z szeregiem popularnych aplikacji i usług internetowych, a także kroki, jakie należałoby przedsięwziąć w celu uniknięcia tych zagrożeń.
- **Opcje ochrony transmisji**
  Tu opisano zabiegi zmierzające do zabezpieczenia danych przepływających przez sieć niezaufaną, taką jak Internet. Opisywane środki zabezpieczeń to połączenia SSL, Client Access Express i połączenia VPN.
- **Wybór opcji ochrony iSeries na poziomie sieci**
  To zwięzłe omówienie opcji zabezpieczających systemu iSeries pozwala wybrać odpowiednią konfigurację do zabezpieczenia systemów i zasobów w zależności od sposobu korzystania z Internetu i strategii e-biznesowej.

Uwaga: Osoby nie znające terminów związanych z ochroną i Internetem mogą w trakcie czytania tej dokumentacji zapoznawać się z sekcją dotyczącą ogólnej terminologii dotyczącej ochrony.

Rozdział 1. Co nowego w wersji V5R1

W wersji V5R1 wprowadzono wiele ulepszeń i dodatków w dziedzinie funkcji ochrony systemu iSeries 400. Poniższa lista opisuje najważniejsze ulepszenia w tym zakresie:

- **Ulepszenia w programie Menedżer certyfikatów cyfrowych (Digital Certificate Manager - DCM)**
  Możliwe jest teraz użycie programu DCM do uzyskiwania certyfikatów, które służą do cyfrowego podpisywania obiektów, i zarządzania tymi certyfikatami. Podpis gwarantuje integralność obiektu i stanowi dowód jego pochodzenia. Ponadto można tworzyć i organizować odpowiednie certyfikaty weryfikujące autentyczność podpisu, za pomocą których użytkownik uwierzytelnia złożony na obiekcie podpis chroniący dane obiektu przed zmianami i dowodzący jego pochodzenia. Program DCM lub odpowiednie funkcje API pozwalają też podpisywać obiekty i sprawdzać autentyczność podpisu obiektów.
- **Cyfrowo podpisany system operacyjny**
  Poczynając od wersji V5R1 system OS/400 i programy licencjonowane IBM będą cyfrowo podpisane przez firmę IBM. Dzięki temu użytkownicy zyskają możliwość sprawdzenia, czy programy te nie zostały zmodyfikowane od czasu ich podpisania przez IBM. Weryfikacja podpisu cyfrowego może być wykonana w czasie odtwarzania lub przez uruchomienie komendy CHKOBJITG. Dostępne są także funkcje API, pozwalające klientom i partnerom handlowym na cyfrowe podpisywanie i weryfikowanie używanych aplikacji.
- **Nowe reguły tworzenia haseł profilu użytkownika (QPWDLVL 2 i 3)**
  Długość hasła profilu użytkownika została zwiększona i może teraz wynosić od 1 do 128 znaków. W hasłach rozróżniane są wielkie i małe litery, a przy tym można w nich stosować spacje. Przykładem prawidłowego hasła jest ″To jest moje nowe hasło″. Spacje dodane na końcu są ignorowane, a poza tym hasło nie może składać się z samych spacji.
- **Usprawnienia dotyczące haseł profilu użytkownika**
  Nowa wartość systemowa QPWDLVL pozwala wybrać jedną z czterech opcji kontrolujących poziom haseł w systemie:
  - PWDLVL 0 — To ustawienie pozwala na stosowanie haseł o długości 10 bajtów oraz na zachowywanie haseł Netserver. Jest to ustawienie domyślne.
  - PWDLVL 1 — To ustawienie pozwala na stosowanie haseł o długości 10 bajtów, lecz nakazuje wyeliminować hasła Netserver.
  - PWDLVL 2 — To ustawienie pozwala na stosowanie haseł o długości 128 znaków oraz na zachowanie haseł spełniających nowe, jak i stare wymagania co do formatu hasła.
  - PWDLVL 3 — To ustawienie pozwala na stosowanie haseł o długości 128 znaków i eliminuje hasła zgodne ze starym formatem.
- **Obsługa koprocesora szyfrującego IBM 4758–023 PCI pozwala na bezpieczniejsze przechowywanie kluczy**
  Jeśli w komputerze zainstalowany jest koprocesor szyfrujący IBM 4758–023 PCI, można go wykorzystać do bezpiecznego przechowywania kluczy do certyfikatu cyfrowego. Podczas tworzenia lub odnawiania certyfikatu za pomocą programu DCM można wybrać między złożeniem kluczy bezpośrednio w koprocesorze a użyciem klucza głównego koprocesora w celu zaszyfrowania klucza prywatnego i zapisania go w specjalnym zbiorze. Przechowywanie kluczy w koprocesorze pozwala ponadto poprawić wydajność protokołu SSL w obsługujących go aplikacjach. Koprocesor sprzętowo wspomaga zadania związane z deszyfrowaniem klucza prywatnego wymaganego podczas uzgadniania inicjującego sesję SSL. Zainstalowanie większej liczby kart 4758 pozwala zrównoważyć ich obciążenie podczas obsługi uzgadniania SSL.
- **Obsługa certyfikatów w sieciach VPN**
  W wersjach wcześniejszych niż V5R1 serwery protokołu IKE (Internet Key Exchange) mogły realizować wzajemne uwierzytelnianie tylko za pomocą klucza wcześniej przekazanego innym sposobem. Procedura ta zapewnia niższy poziom bezpieczeństwa, ponieważ wcześniej wymagane jest samodzielne przekazanie klucza administratorowi systemu na drugim końcu połączenia VPN. Istnieje przy tym możliwość, że klucz w trakcie przekazywania zostanie przechwycony przez niepowołane osoby. W wersji V5R1 niebezpieczeństwa tego można uniknąć, uwierzytelniając punkt końcowy połączenia za pomocą

cyfrowego certyfikatu zamiast klucza. Do zarządzania certyfikatami używanymi przez serwer IKE do zestawiania dynamicznych połączeń VPN służy program Menedżer certyfikatów cyfrowych (Digital Certificate Manager - DCM).

- **Usprawnienia dotyczące aplikacji obsługujących SSL**
  W wersji V5R1 wprowadzono wiele usprawnień w korzystaniu z protokołu SSL. Możliwe jest teraz skonfigurowanie serwera FTP iSeries na potrzeby sesji komunikacyjnych chronionych przez SSL. Serwer FTP może korzystać z certyfikatów cyfrowych do uwierzytelniania klientów. Dodatkowo, w wersji V5R1 systemu OS/400 wprowadzono obsługę 128-bitowego algorytmu szyfrowania AES. Jest to nowy, szybszy algorytm, który zastąpił stosowany wcześniej algorytm DES.
- **Usprawnienia dotyczące protokołu pocztowego SMTP**
  Serwer SMTP obsługuje obecnie funkcję listy zastrzeżeń bazującej na treści pól zawierających temat, nadawcę i adres IP.
- **Kreator konfiguracji internetowej**
  Popularny Kreator konfiguracji internetowej, dostępny w poprzedniej wersji jako oddzielny plik do pobrania, teraz stanowi jeden ze standardowych elementów programu Operations Navigator. Kreator ten pozwala automatycznie konfigurować połączenie z Internetem dla systemu iSeries oraz zabezpieczyć to połączenie przez zastosowanie automatycznie wygenerowanych reguł filtrowania pakietów.
- **Usprawnienia dotyczące przechowywania danych na potrzeby odtwarzania programów**
  Programy utworzone dla systemów iSeries w wersji V5R1 zawierają informacje pozwalające na ewentualne ponowne utworzenie programu w trakcie operacji odtwarzania. Informacje niezbędne w celu ponownego utworzenia programu pozostają związane z programem nawet po wyeliminowaniu jego obserwowalności. Jeśli w trakcie odtwarzania programu wykryty zostanie błąd potwierdzenia, program zostanie ponownie utworzony w celu usunięcia przyczyn błędu. Operacja ponownego tworzenia programu w trakcie odtwarzania nie jest nowością w systemie iSeries w wersji V5R1. W poprzednich wersjach wszelkie błędy potwierdzenia programu, napotkane w trakcie odtwarzania, także powodowały ponowne utworzenie programu, pod warunkiem że było to możliwe, tzn. gdy odtwarzany program był obserwowalny. Różnica w systemie iSeries w wersji V5R1 polega na tym, że informacje potrzebne do ponownego utworzenia programu pozostają, nawet gdy program nie jest już obserwowalny. W efekcie, każdy program utworzony dla wersji V5R1 lub późniejszej, dla którego w trakcie odtwarzania zaistnieją błędy potwierdzenia, zostanie ponownie utworzony z usunięciem zmian będących przyczyną błędu.

Rozdział 2. Drukowanie tego dokumentu

Aby obejrzeć lub wydrukować ten dokument, można go pobrać w postaci pliku w formacie PDF. Aby móc przeglądać dokumenty w formacie PDF, konieczne jest zainstalowanie przeglądarki Adobe Acrobat Reader.

Kopię programu można pobrać ze strony głównej Adobe. 

Aby przejrzeć lub pobrać wersję dokumentu w formacie PDF, wybierz odsyłacz IBM SecureWay: iSeries a Internet (416 kB lub 60 stron).

Aby zapisać plik PDF na stacji roboczej w celu oglądania lub drukowania:
1. Otwórz plik PDF w oknie przeglądarki (kliknij powyższy odsyłacz).
2. W menu przeglądarki kliknij **Plik**.
3. Kliknij **Zapisz jako...**
4. Wybierz katalog, w którym chcesz zapisać plik PDF.
5. Kliknij **Zapisz**.

Rozdział 3. iSeries 400 a ochrona internetowa

Gdy właściciel systemu iSeries 400 bada możliwości łączenia swoich systemów z Internetem, zwykle zadaje sobie pytanie: ″Jak rozpocząć korzystanie z Internetu w celach biznesowych?″, następnie: ″Co trzeba wiedzieć o ochronie i Internecie?″. W tej sekcji spróbujemy odpowiedzieć na drugie pytanie.

Odpowiedź na pytanie: ″Co trzeba wiedzieć o ochronie i sieci Internet?″ zależy od sposobu użytkowania Internetu. Zagadnienia ochrony związane z Internetem są bardzo ważne. Które zagadnienia należy uwzględnić, zależy od sposobów korzystania z sieci. Pierwszym kontaktem z Internetem może być zapewnienie użytkownikom sieci wewnętrznej dostępu do sieci WWW i internetowej poczty elektronicznej. Może być również potrzebne przesyłanie ważnych informacji z jednego punktu do innego. Internet można też wykorzystać do handlu elektronicznego lub do utworzenia sieci extranet pomiędzy firmą a jej partnerami handlowymi i dostawcami.

Przed rozpoczęciem korzystania z Internetu należy zdecydować, do czego Internet będzie służył i w jaki sposób będzie się go użytkować. Podjęcie decyzji dotyczących używania Internetu i ochrony internetowej może być złożonym procesem. Podczas opracowywania własnych planów wykorzystania Internetu, warto przejrzeć sekcję Scenariusz: plany biznesu elektronicznego firmy JKL Toy Company. (Uwaga: osoby nie znające terminów związanych z ochroną i Internetem mogą w trakcie czytania tej dokumentacji zapoznawać się z sekcją dotyczącą ogólnej terminologii dotyczącej ochrony).

Do opracowania własnych celów i strategii ochrony konieczne jest ustalenie metod korzystania z Internetu i prowadzenia e-biznesu, zrozumienie zagadnień związanych z ochroną i poznanie dostępnych narzędzi, ich funkcji i ofert ochrony. Na decyzje dotyczące strategii ochrony wpływa wiele czynników. Po rozszerzeniu obszaru zainteresowania organizacji na Internet strategia ochrony staje się fundamentem należytego zabezpieczenia posiadanych systemów i zasobów.

Charakterystyka ochrony systemu iSeries 400

Niezależnie od funkcji specjalnie przeznaczonych do ochrony systemu od strony Internetu, iSeries 400 charakteryzuje się bardzo wysokim poziomem bezpieczeństwa ogólnego dzięki następującym czynnikom:

- Zintegrowana ochrona, bardzo trudna do obejścia w porównaniu z ochroną innych systemów, opartą na dodatkowych pakietach oprogramowania.
- Oparta na obiektach architektura powoduje, że tworzenie i rozprzestrzenianie się wirusów jest trudne technicznie. W systemie iSeries plik nie może udawać programu ani zmieniać innego programu. Opcje integralności iSeries wymagają używania dostarczanych z systemem interfejsów do uzyskiwania dostępu do obiektów. Nie można uzyskiwać dostępu do obiektów bezpośrednio za pomocą ich adresu w systemie. Nie można pobrać offsetu (przesunięcia) i zamienić go we wskaźnik ani samodzielnie utworzyć wskaźnika. Manipulacja wskaźnikami jest popularną techniką używaną przez hakerów w innych systemach.
- Elastyczność pozwala ustawić ochronę systemu w sposób zgodny ze specyficznymi wymaganiami.

  Można skorzystać z usług programu Security Advisor, w Technical Studio, który pomoże dobrać parametry ochrony najbardziej dopasowane do potrzeb konkretnego systemu.

Zaawansowane funkcje ochrony w iSeries

iSeries zawiera także kilka ofert ochrony mających na celu rozszerzenie ochrony systemu podczas podłączania go do Internetu. W zależności od sposobu używania Internetu można korzystać z:

- Sieci VPN, które są rozszerzeniem prywatnej sieci intranet firmy na sieć publiczną, na przykład na Internet. Sieci VPN można używać do tworzenia chronionych połączeń prywatnych, polegających na tworzeniu prywatnego ″tunelu″ w sieci publicznej. Sieć VPN to wbudowana opcja systemu OS/400 dostępna z interfejsu Operations Navigator.

- Reguły pakietów to wbudowana funkcja systemu OS/400, dostępna za pośrednictwem interfejsu programu Operations Navigator. Funkcja ta pozwala na skonfigurowanie filtru pakietów IP i reguł translacji adresów sieciowych w celu sterowania przepływem przychodzących i wychodzących pakietów TCP/IP w systemie iSeries.
- Ochrona komunikacji aplikacji SSL umożliwia skonfigurowanie aplikacji do korzystania z protokołu SSL podczas ustanawiania chronionych połączeń pomiędzy aplikacjami serwera i ich klientami. Protokół SSL pierwotnie był przeznaczony dla chronionych przeglądarek WWW i aplikacji serwera, ale mogą go wykorzystywać także inne aplikacje. Wiele spośród aplikacji systemu iSeries ma obecnie możliwość korzystania z protokołu SSL. Należą do nich takie aplikacje, jak IBM HTTP Server for iSeries, Client Access Express, File Transfer Protocol (FTP), Telnet i wiele innych.

Do opracowania własnych celów i strategii ochrony konieczne jest ustalenie metod korzystania z Internetu, zrozumienie zagadnień związanych z ochroną i poznanie dostępnych narzędzi, ich funkcji i oferty ochrony. Na decyzje dotyczące strategii ochrony wpływa wiele czynników. Po rozszerzeniu obszaru zainteresowania organizacji na Internet strategia ochrony stała się fundamentem chronienia systemu.

Uwaga: Aby znaleźć bardziej szczegółowe informacje na temat rozpoczęcia korzystania z Internetu w celach biznesowych, należy przejrzeć następujące zagadnienia Centrum informacyjnego i dokumentacji technicznej IBM (Redbooks):
- *Połączenie z Internetem*
- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929). 

Rozdział 4. Planowanie ochrony internetowej

Podczas opracowywania planu użytkowania Internetu należy dokładnie zaplanować ochronę internetową. Należy zgromadzić szczegółowe informacje na temat planowanego sposobu korzystania z Internetu oraz udokumentować konfigurację sieci wewnętrznej. W oparciu o tak zebrane informacje można precyzyjnie określić istniejące potrzeby w zakresie ochrony sieci.

Na przykład należy udokumentować i opisać informacje dotyczące poniższych kwestii:
- aktualnej konfiguracji sieci,
- informacji o konfiguracji serwera DNS czy poczty elektronicznej,
- połączenia z dostawcą usług internetowych,
- rodzaju potrzebnych usług internetowych,
- rodzaju usług oferowanych użytkownikom Internetu.

Udokumentowane informacje tego typu są pomocne przy określaniu części systemu podatnych na atak i środków ochrony, które są niezbędne do zminimalizowania tych zagrożeń.

Załóżmy, że podjęto decyzję, iż użytkownicy sieci wewnętrznej mogą korzystać z usługi Telnet podczas łączenia się z hostami w ośrodku badawczym. Potrzebują tej usługi do tworzenia nowych produktów dla firmy. Pojawia się jednak problem poufnych danych płynących przez sieć Internet bez żadnej ochrony. Jeśli konkurencja przechwyci i wykorzysta dane, to firma może stanąć w obliczu zagrożenia finansowego. Po określeniu potrzeb (Telnet) i związanych z nimi niebezpieczeństw (ujawnienie poufnych danych) możliwe jest określenie, jakie dodatkowe środki ochrony należy podjąć, aby zapewnić poufność danych (obsługa SSL).

Po opracowaniu planu użytkowania Internetu i planów ochrony należy przeczytać następujące sekcje:
- **Warstwowa obrona - podejście do ochrony** zawiera informacje o problemach związanych z tworzeniem wszechstronnego planu ochrony.
- **Cele i strategie ochrony** zawiera informacje pomagające lepiej pojąć zagadnienia związane z tworzeniem kompleksowego planu ochrony.
- **Przykład: plany JKL Toy Company w zakresie e-biznesu** zawiera praktyczny przykład typowego wykorzystania Internetu przez firmę i plany ochrony, które można wykorzystać przy tworzeniu własnych strategii.

Mimo że produkt IBM Firewall for AS/400 nie jest już oferowany, nadal celowe może być adaptowanie i wykorzystywanie do własnych celów związanych z nim arkuszy planowania. Arkusze planowania pomogą zebrać ważne i szczegółowe informacje na temat planów użytkowania Internetu i oszacować potrzeby ochrony. Arkusze są dostępne w dokumencie Firewall: Pierwsze kroki w Centrum informacyjnym iSeries dla wersji V4R5. Bez względu na to, czy zdecydowano się korzystać z firewalla, czy nie, i tak trzeba zgromadzić te same dane, aby zaplanować strategię ochrony internetowej.

Warstwowa obrona - podejście do ochrony

Strategia ochrony definiuje obiekt ochrony i oczekiwania wobec użytkowników systemu. Stanowi podstawę niezbędną do planowania ochrony podczas projektowania nowych aplikacji lub rozszerzania posiadanej sieci. Opisuje zakres odpowiedzialności użytkownika, na przykład za ochronę poufnych informacji lub tworzenie haseł, które nie są łatwe do odgadnięcia.

Uwaga: Należy opracować i wprowadzić taką strategię ochrony organizacji, która minimalizuje zagrożenia dla sieci wewnętrznej. Poprawnie skonfigurowane opcje ochrony, wbudowane w system iSeries 400, pozwalają zminimalizować wiele zagrożeń. Gdy system iSeries zostanie podłączony do Internetu, potrzebne jest podjęcie dodatkowych kroków w celu zapewnienia ochrony sieci wewnętrznej.

Prowadzenie biznesu poprzez Internet niesie wiele zagrożeń. Tworząc strategię ochrony, należy zrównoważyć możliwość świadczenia usług i kontrolowania dostępu do funkcji i danych. W przypadku komputerów w sieci ochrona jest trudniejsza, ponieważ kanał komunikacyjny jest otwarty na atak.

Niektóre usługi internetowe są szczególnie podatne na pewne typy ataków. Z tego względu sprawą kluczowej wagi jest zdanie sobie sprawy z zagrożeń związanych z każdą usługą, która będzie używana lub udostępniana. Ponadto znajomość możliwych zagrożeń pozwala na zdefiniowanie zbioru precyzyjnych celów ochrony.

Niektórzy użytkownicy Internetu świadomie próbują zagrozić bezpieczeństwu komunikacji poprzez Internet. Poniższa lista opisuje kilka typowych zagrożeń:

- **Ataki pasywne**: Podczas ataku pasywnego intruz ogranicza się do obserwacji ruchu w sieci, usiłując zdobyć poufne informacje. Takie ataki mogą następować w sieci (śledzenie łącza komunikacyjnego) lub w systemie (zastąpienie komponentu systemowego koniem trojańskim, który podstępnie przechwytuje dane). Bardzo trudno wykryć ataki pasywne. Dlatego też należy założyć, że wszystkie dane przesyłane przez Internet są przez kogoś przechwytywane.
- **Ataki aktywne:** Podczas ataku aktywnego intruz usiłuje złamać zabezpieczenia systemu i dostać się do systemów w sieci. Istnieje kilka rodzajów ataków aktywnych:
  - **Próby dostępu do systemu** - napastnik usiłuje wykorzystać luki w ochronie, aby uzyskać dostęp i przejąć kontrolę nad systemem klienta lub serwera.
  - **Oszukiwanie** - napastnik próbuje przedostać się przez obronę podszywając się pod użytkownika lub system zaufany, a później skłonić system do przesłania mu tajnych informacji.
  - **Odmowa usługi** - napastnik próbuje zakłócić lub zakończyć działanie systemu zmieniając kierunek przepływu danych w sieci lub bombardując system śmieciami.
  - **Atak kryptograficzny** - napastnik próbuje zgadnąć lub wykraść hasło albo korzysta ze specjalizowanych narzędzi próbując deszyfrować zaszyfrowane dane.

Wielowarstwowa obrona

Potencjalne zagrożenia w Internecie mogą wystąpić na różnych poziomach, dlatego niezbędne jest zastosowanie wielu warstw ochrony przeciwko tym zagrożeniom. Ogólnie ujmując, przy łączeniu z Internetem nie należy się zastanawiać, **czy wystąpią** próby włamania do systemu lub ataki typu odmowa usługi. Należy z góry założyć, że problemy tego typu **na pewno wystąpią**. Najlepszą obroną jest zatem przemyślany, uprzedzający zagrożenia atak. Skorzystanie z podejścia warstwowego podczas planowania strategii ochrony internetowej zapewnia, że intruz, który przedrze się przez pierwszą warstwę obrony, zostanie zatrzymany przez następną warstwę.

Strategia ochrony powinna zawierać środki ochrony w poszczególnych warstwach tradycyjnego modelu przetwarzania sieciowego. Podsumowując, ochronę należy planować od najprostszej (ochrona na poziomie systemu) do najbardziej złożonej (ochrona na poziomie transakcji).

Ochrona na poziomie systemu

Środki ochrony systemu stanowią ostatnią linię obrony przed próbami dostępu do systemu poprzez Internet. Dlatego też pierwszym punktem w kompleksowej strategii ochrony internetowej musi być prawidłowe skonfigurowanie podstawowych ustawień ochrony systemu iSeries.

Ochrona na poziomie sieci

Środki ochrony sieci sterują dostępem do systemu iSeries i do innych systemów w sieci. Gdy sieć zostaje podłączona do Internetu, należy upewnić się, że zastosowany jest odpowiedni poziom ochrony sieci, który pozwoli zabezpieczyć zasoby wewnętrznej sieci przed nieautoryzowanym dostępem i wtargnięciem. Najczęściej stosowane jest rozwiązanie oparte na firewallu. Dostawca usług internetowych może i powinien stanowić ważny element w planie ochrony sieci. Schemat ochrony sieciowej powinien informować, jakie środki

ochrony są dostarczane przez dostawcę usług internetowych, np reguły filtrowania dla połączeń z routerem dostawcy usług internetowych i środki ostrożności dotyczące publicznej usługi DNS.

Ochrona na poziomie aplikacji
Środki ochrony na poziomie aplikacji sterują interakcją użytkownika z określonymi aplikacjami. Należy skonfigurować ustawienia ochrony dla każdej używanej aplikacji. Szczególny nacisk należy położyć na ustawienie tych aplikacji, które będą używane lub dostarczane do Internetu. Takie aplikacje i usługi są narażone na nieprawidłowe użycie przez nieuprawnionych użytkowników szukających dostępu do systemów sieciowych. Wybrane środki ochrony powinny obejmować zagrożenia zarówno po stronie klienta, jak i serwera.

Ochrona na poziomie transmisji
Środki ochrony na poziomie transmisji zabezpieczają przesyłanie danych przez sieć i między sieciami. Podczas komunikacji przez niezaufaną sieć, taką jak Internet, nie ma możliwości sprawdzenia przepływu pakietów od nadawcy do odbiorcy. Pakiety oraz dane, które przenoszą, przepływają przez wiele różnych serwerów i nie ma nad nimi kontroli. Jeśli nie zostaną ustawione środki ochrony, takie jak na przykład korzystanie przez aplikacje z protokołu SSL, przepływające dane będą dostępne dla każdego, każdy będzie mógł je przejrzeć i wykorzystać. Środki ochrony na poziomie transmisji zabezpieczają dane przepływające pomiędzy granicami innych poziomów ochrony.

Tworząc ogólną strategię ochrony w Internecie należy utworzyć taką strategię osobno dla każdej warstwy. Ponadto należy opisać, jak każdy zestaw strategii współpracuje z innymi przy zapewnianiu bezpiecznej sieci dla potrzeb firmy.

Cele i strategie ochrony

Strategia ochrony

Użycie bądź udostępnienie dowolnej usługi internetowej stwarza zagrożenie dla systemu iSeries i sieci, z którą jest on połączony. Strategia ochrony to zestaw reguł dotyczących czynności związanych z zasobami komunikacyjnymi i komputerowymi należącymi do jednej organizacji. Reguły te obejmują takie zagadnienia, jak ochrona fizyczna, ochrona personelu, ochrona administracyjna i ochrona sieci.

Strategia ochrony definiuje obiekt ochrony i oczekiwania wobec użytkowników systemu. Stanowi podstawę niezbędną do planowania ochrony podczas projektowania nowych aplikacji lub rozszerzania posiadanej sieci. Opisuje zakres odpowiedzialności użytkownika, na przykład za ochronę poufnych informacji lub tworzenie haseł, które nie są łatwe do odgadnięcia. Strategia ochrony powinna też określać sposób monitorowania skuteczności podjętych zabiegów. Stałe monitorowanie tego typu pozwala wykrywać na bieżąco podejmowane próby obejścia zastosowanych zabezpieczeń.

Aby opracować własną strategię ochrony, należy precyzyjnie zdefiniować cele ochrony. Po utworzeniu strategii ochrony należy podjąć kroki w celu wdrożenia reguł zawartych w strategii. Kroki te obejmują szkolenie pracowników oraz instalację sprzętu i oprogramowania niezbędnego do wdrożenia tych reguł. Ponadto, gdy wprowadzane są zmiany w środowisku przetwarzania, należy aktualizować strategię ochrony, aby zapewnić identyfikację i neutralizację zagrożeń związanych z wprowadzonymi zmianami. Przykład strategii ochrony dla firmy JKL Toy Company można znaleźć w Centrum informacyjnym iSeries w sekcji Planowanie ochrony i ochrona systemu - podstawy.

Cele strategii

Podczas tworzenia i wdrażania strategii ochrony należy precyzyjnie określić jej cele. Cele ochrony należą do jednej lub kilku wymienionych kategorii:

Ochrona zasobów

Zapewnia dostęp do zasobów systemu tylko uprawnionym użytkownikom. Mocną stroną iSeries jest możliwość ochrony wszystkich typów zasobów systemowych. Należy dokładnie zdefiniować kategorie użytkowników mających dostęp do systemu. W ramach tworzenia strategii ochrony należy także zdefiniować uprawnienia dostępu, jakie będą miały grupy użytkowników.

Uwierzytelnianie

Pewność lub sprawdzenie, czy zasób (człowiek lub komputer) znajdujący się po drugiej stronie sesji rzeczywiście jest tym, za kogo się podaje. Niezawodne uwierzytelnianie chroni system przed użytkownikami, którzy - używając fałszywych danych identyfikacyjnych - usiłują uzyskać dostęp do systemu. Do uwierzytelniania system zwykle wykorzystuje nazwy i hasła użytkowników; bezpieczniejszą metodą są certyfikaty cyfrowe, które ponadto przynoszą inne korzyści. Po podłączeniu systemu do sieci publicznej, takiej jak Internet, uwierzytelnianie użytkowników uzyskuje nowy wymiar. Istotną różnicą pomiędzy siecią Internet i intranet jest to, że można mieć zaufanie do podanej tożsamości użytkownika wpisującego się do systemu. Dlatego też należy wziąć pod uwagę używanie lepszych metod uwierzytelniania, niż tradycyjne sprawdzanie nazwy użytkownika i hasła podczas logowania. Uwierzytelnieni użytkownicy mogą mieć różne typy uprawnień, w zależności od nadanych im poziomów uprawnień.

Nadawanie uprawnień

Pewność, że osoba lub komputer znajdujący się po drugiej stronie sesji ma uprawnienia do wykonania żądania. Nadawanie uprawnień to proces określania, kto lub co może uzyskać dostęp do zasobu systemu lub wykonać w systemie określoną czynność. Zazwyczaj nadawanie uprawnień jest częścią uwierzytelniania.

Integralność

Pewność, że napływające informacje są identyczne z wysłanymi. Zrozumienie integralności wymaga zrozumienia koncepcji integralności danych i integralności systemu.

- **Integralność danych**: Dane są zabezpieczone przed nieuprawnionymi zmianami lub manipulacjami. Integralność danych chroni przed niebezpieczeństwem manipulacji, polegającym na nieuprawnionym przechwytywaniu i zmienianiu informacji. Oprócz ochrony danych przechowywanych w sieci może być potrzebna dodatkowa ochrona w celu zapewnienia integralności podczas wprowadzania danych do systemu z niezaufanego źródła. Jeśli napływające do systemu dane pochodzą z sieci publicznej, mogą być potrzebne metody ochrony, które pozwolą:
  - chronić dane przed “węszeniem” (sniffing) i interpretacją; w tym celu zwykle korzysta się z szyfrowania,
  - upewniać się, że transmisja nie została zmieniona (integralność danych),
  - udowadniać, że transmisja miała miejsce (nieodrzucanie); w przyszłości może być potrzebny elektroniczny odpowiednik listu poleconego.
- **Integralność systemu**: System dostarcza spójnych, oczekiwanych wyników przy zachowaniu spodziewanej wydajności. W iSeries integralność systemu jest łatwym do przeoczenia komponentem systemu, dlatego że jest podstawową częścią architektury iSeries. Przykładowo, architektura iSeries sprawia, że przy poziomie ochrony równym 40 lub 50 imitowanie lub modyfikowanie programu systemu operacyjnego staje się wyjątkowo trudne.

Nieodrzucanie

Nieodrzucanie (non-repudiation) jest dowodem na to, że transakcja miała miejsce albo że komunikat został wysłany lub odebrany. Korzystanie z certyfikatów cyfrowych lub szyfrowania według klucza publicznego w celu ″podpisywania″ transakcji, komunikatów i dokumentów zapewnia nieodrzucanie. Zarówno nadawca, jak i odbiorca zgadzają się, że odbyła się wymiana. Za dowód wystarcza opatrzenie danych cyfrowym podpisem.

Tajność

Pewność, że tajne informacje pozostają prywatne i nie są widoczne dla podglądaczy.

Poufność jest kluczowym elementem pełnej ochrony danych. Szyfrowanie danych za pomocą certyfikatów cyfrowych i protokół SSL pomaga zapewnić poufność danych podczas przesyłania ich przez sieci niezaufane. Strategia ochrony powinna określać sposób ochrony poufności informacji wewnątrz sieci lokalnej i po jej wyjściu z sieci.

Kontrola działania ochrony
Monitorowanie zdarzeń dotyczących ochrony w celu protokołowania pomyślnych i niepomyślnych (odrzuconych) prób dostępu. Zapisy pomyślnie zakończonych prób dostępu informują o wykonywanych w systemie czynnościach i zachowaniu użytkowników. Zapisy niepomyślnie zakończonych (odrzuconych) prób dostępu informują o próbach przełamania ochrony lub trudnościach z uzyskaniem dostępu do systemu.

Zrozumienie celów ochrony pomaga utworzyć strategię ochrony obejmującą wszystkie potrzeby ochrony internetowej i ochrony sieci. Pomocne może być przeczytanie podczas definiowania celów i tworzenia własnych strategii ochrony scenariusza biznesu elektronicznego firmy JKL Toy Company. Opisane w przykładzie wykorzystanie Internetu i plan ochrony odpowiada wielu rzeczywistym implementacjom.

Scenariusz: plany biznesu elektronicznego firmy JKL Toy Company

Scenariusz opisuje typową firmę. JKL Toy Company zdecydowała się na rozszerzenie swoich celów biznesowych na Internet. Wprawdzie firma jest fikcyjna, jednak jej plany wykorzystania Internetu dla potrzeb biznesu elektronicznego i określone w rezultacie potrzeby ochrony są reprezentatywne dla sytuacji wielu firm, istniejących w rzeczywistym świecie.

Firma JKL Toy Company jest małą, ale szybko powiększającą się firmą wytwarzającą zabawki, od latawców po przytulanki. Prezes firmy stara się zapewnić rozwój firmy wykorzystując do tego celu system iSeries. Za administrację systemu iSeries i ochronę systemu odpowiedzialna jest Sharon Jones - kierownik działu księgowości.

Firma od lat z powodzeniem korzysta ze swojej strategii ochrony wewnętrznych aplikacji. Obecnie planowane jest użycie intranetu do efektywniejszej wewnętrznej komunikacji. Ponadto firma rozważa możliwość wykorzystania Internetu dla celów biznesowych. W planach jest wykreowanie wizerunku firmy w Internecie, włącznie z utworzeniem katalogu elektronicznego oraz wykorzystanie Internetu do transmisji ważnych danych ze zdalnych miejsc do biura korporacji. Ponadto firma chce zapewnić pracownikom laboratorium projektów dostęp do Internetu dla celów badawczych i projektowych. Poza tym firma chce umożliwić klientom korzystanie z własnego serwisu WWW do składania bezpośrednich zamówień. Sharon tworzy raport o możliwych specyficznych zagrożeniach związanych z taką działalnością i o tym, jakie środki ochrony powinna podjąć firma, aby zminimalizować te zagrożenia. Będzie ona odpowiedzialna za zaktualizowanie firmowej strategii ochrony i zastosowanie w praktyce środków ochrony, które firma zdecyduje się zastosować.

Cele rozszerzenia obecności w Internecie:
- promowanie ogólnego wizerunku firmy i jej reprezentacji jako część ogólnej kampanii reklamowej,
- dostarczanie katalogu produktów online dla klientów i personelu sprzedaży,
- poprawienie obsługi klienta,
- umożliwienie pracownikom dostępu do poczty elektronicznej i sieci WWW.

Upewniwszy się, że wdrożono należytą podstawową ochronę systemu iSeries, firma JKL Toy postanowiła użyć firewalla, aby zapewnić ochronę na poziomie sieci. Firewall będzie chronić sieć wewnętrzną przed wieloma potencjalnymi zagrożeniami związanymi z Internetem. Poniżej przedstawiono konfigurację Internetu w firmie.

Jak wynika z ilustracji, w firmie JKL działają dwa podstawowe systemy iSeries. Jeden system jest wykorzystywany dla potrzeb aplikacji projektowych (JKLDEV), a drugi dla potrzeb aplikacji produkcyjnych

(JKLPROD). Oba systemy obsługują dane i aplikacje o znaczeniu krytycznym. Dlatego też nie jest wskazane uruchamianie aplikacji internetowych na tych systemach. W celu uruchomienia tych aplikacji podjęto więc decyzję o dodaniu kolejnego systemu iSeries (JKLINT).

Nowy system umieszczono w sieci obwodowej. Pomiędzy nim a wewnętrzną siecią firmową umieszczono firewall, aby zapewnić lepszą separację własnej sieci od Internetu. Separacja ta zmniejsza niebezpieczeństwo ze strony sieci Internet, na które narażone są systemy wewnętrzne. Przeznaczając nowy system iSeries tylko do obsługi sieci Internet, firma zmniejsza złożoność ochrony sieci.

Firma nie uruchamia teraz na nowym systemie iSeries żadnych aplikacji o znaczeniu krytycznym. Na tym etapie planów biznesu elektronicznego nowy system stanowi jedynie statyczny publicznie dostępny serwis WWW. Jednak firma chce zaimplementować środki ochrony, aby zabezpieczyć system i uruchomiony, publicznie dostępny, serwis WWW przed przerwaniem działania usługi czy innymi możliwymi atakami. Dlatego firma będzie zabezpieczać system zarówno za pomocą reguł filtrowania pakietów i reguł translacji adresu sieciowego, jak i podstawowych środków ochrony.

W miarę jak firma będzie dostarczała bardziej zaawansowanych aplikacji dostępnych publicznie (handel elektroniczny czy dostęp w sieci extranet) implementowane będą bardziej zaawansowane środki ochrony.

Rozdział 5. Poziomy ochrony dla podstawowego zakresu gotowości internetowej

Środki ochrony systemu stanowią ostatnią linię obrony przed próbami dostępu do systemu poprzez Internet. Dlatego też pierwszym punktem w kompleksowej strategii ochrony internetowej musi być prawidłowe skonfigurowanie podstawowych ustawień ochrony systemu OS/400. Aby upewnić się, że system spełnia minimalne wymagania ochrony, trzeba wykonać poniższe czynności:

- Ustaw poziom ochrony (wartość systemowa QSECURITY) na 50. Wartość 50 zapewnia najwyższy stopień ochrony integralności danych, co jest zdecydowanie zalecane podczas pracy w środowiskach o wysokim poziomie ryzyka, do których należy Internet.

  Uwaga: W przypadku aplikacji pracujących głównie w modelu transakcyjnym lub intensywnie korzystających z systemu plików IFS (Integrated File System) praca przy poziomie ochrony o wartości 50 może prowadzić do obniżenia wydajności.

  Więcej informacji na temat poszczególnych poziomów ochrony w systemie iSeries można znaleźć w dokumencie Wskazówki i narzędzia dotyczące ochrony iSeries.

  Uwaga: Jeśli aktualnie ustawiony jest poziom ochrony niższy niż 50, to może wystąpić potrzeba aktualizacji procedur operacyjnych albo aplikacji. Wskazane jest zapoznanie się z informacjami zawartymi w książce iSeriesSecurity Reference przed zmianą poziomu ochrony na wyższy.
- Należy ustawić wartości systemowe dotyczące ochrony na co najmniej tak restrykcyjne, jak zalecane ustawienia. W celu porównania istniejących ustawień z zalecanymi można posłużyć się Kreatorem ochrony z programu Operations Navigator lub Security Advisor z Technical Studio.
- Należy upewnić się, że żaden profil użytkownika, w tym profile użytkowników dostarczone przez IBM, nie ma hasła domyślnego. Aby to sprawdzić, należy użyć komendy Analiza domyślnych haseł (Analyze Default Passwords - ANZDFTPWD).
- Aby chronić ważne zasoby systemowe, należy korzystać z uprawnień do obiektów. Należy zastosować restrykcyjne podejście do systemu. Oznacza to, że domyślnie nikt (PUBLIC *EXCLUDE) nie powinien mieć praw do zasobów systemowych, takich jak biblioteki i katalogi. Na dostęp do tych zasobów można zezwolić jedynie kilku użytkownikom. W środowisku Internetu ograniczenie dostępu za pomocą menu nie jest wystarczające.
- **Koniecznie** trzeba ustawić uprawnienia do obiektów w systemie. Więcej informacji na ten temat można znaleźć w rozdziale dotyczącym iSeries Navigator w książce Wskazówki i narzędzia dotyczące ochrony iSeries .

Do pomocy w skonfigurowaniu tych minimalnych wymagań ochrony systemowej można użyć opcji **Security Advisor** (dostępnej z serwisu WWW Technical Studio) lub **Kreatora ochrony** (dostępnego z interfejsu iSeries Navigator). Security Advisor w Technical Studio generuje zestaw zaleceń dotyczących ochrony w oparciu o odpowiedzi użytkownika na szereg zadanych pytań. Z zaleceń tych można skorzystać podczas konfigurowania ustawień ochrony systemowej odpowiednio do potrzeb. Kreator ochrony działa na tej samej zasadzie. W przeciwieństwie do opcji Security Advisor, kreator może automatycznie skonfigurować ustawienia ochrony.

Poprawnie skonfigurowane wbudowane opcje ochrony systemu iSeries umożliwiają minimalizację wielu zagrożeń. Jednak gdy system iSeries zostanie podłączony do Internetu, potrzebne będzie podjęcie dodatkowych kroków w celu zapewnienia ochrony sieci wewnętrznej. Po upewnieniu się, że system iSeries ma dobry ogólny poziom ochrony systemowej, należy skonfigurować dodatkowe środki ochrony, co stanowi część wszechstronnego planu ochrony w celu wykorzystania Internetu.

Rozdział 6. Ochrona na poziomie sieci

Przy łączeniu się z niezaufaną siecią, strategia ochrony musi opisywać całkowity schemat ochrony, w tym opis środków, które zostaną zaimplementowane na poziomie sieci. Jednym z lepszych sposobów dostarczenia pełnego zestawu środków ochrony na poziomie sieci jest zainstalowanie firewalla.

Ponadto dostawca usług internetowych może i powinien stanowić ważny element w planie ochrony sieci. Schemat ochrony sieciowej powinien zawierać dane o tym, jakie środki ochrony są dostarczane przez dostawcę usług internetowych, np. reguły filtrowania dla połączeń z routerem dostawcy usług internetowych oraz środki ostrożności dotyczące publicznej usługi DNS.

Jakkolwiek firewall w ogólnym planie zabezpieczenia systemu z pewnością stanowi jedną z głównych linii obrony, nie powinien być **jedyną** linią obrony. Potencjalne zagrożenia w Internecie mogą wystąpić na różnych poziomach, dlatego niezbędne jest zastosowanie wielu środków ochrony przeciwko tym zagrożeniom.

Firewall w znacznym stopniu uodparnia system na niektóre rodzaje ataków, lecz powinien być tylko jednym z elementów kompleksowego programu ochrony. Na przykład firewall nie zapewnia ochrony danych wysyłanych poprzez Internet w aplikacjach, takich jak poczta SMTP, usługi FTP lub sesje TELNET. Jeśli dane te nie zostaną przed wysłaniem poddane szyfrowaniu, osoba o złych intencjach może przechwycić je na drodze do miejsca przeznaczenia.

Przyłączając sieć wewnętrzną lub system iSeries do Internetu należy zawsze poważnie rozważyć zastosowanie firewalla jako głównej linii obrony przeciwko atakom. Wprawdzie produkt IBM Firewall for AS/400 nie jest już oferowany i obsługiwany, na rynku dostępnych jest wiele innych produktów pełniących analogiczne funkcje.

Więcej informacji na temat zamiany zainstalowanego produktu IBM Firewall for AS/400 na inny produkt podobnego typu lub przejścia na funkcje ochrony sieci wbudowane w serwer iSeries można znaleźć w dokumencie All You Need to Know When Migrating from IBM Firewall for AS/400  (SG24-6152).

Ponieważ na rynku oferowanych jest wiele atrakcyjnych systemów zapór sieciowych, firma JKL Toy Company, aby zabezpieczyć swoją sieć wewnętrzną, zdecydowała się na zakup jednego z nich w ramach wdrażania systemu ochrony działalności e-biznesowej. Jednak wybrany firewall nie zapewnia żadnej ochrony nowemu serwerowi internetowemu iSeries. Dlatego postanowiono dodatkowo zainstalować opcję reguł pakietów w iSeries, aby utworzyć filtry i reguły translacji adresów sieciowych do sterowania przepływem pakietów dla serwera internetowego.

Informacje o regułach pakietów w iSeries

Reguły filtrowania pakietów pozwalają zabezpieczyć systemy komputerowe przez odrzucanie lub akceptowanie pakietów IP w zależności od zdefiniowanego kryterium. Reguły translacji adresów sieciowych umożliwiają ukrycie informacji z systemu wewnętrznego przed użytkownikami z zewnątrz poprzez zamianę jednego adresu IP na inny, publiczny. Wprawdzie filtrowanie pakietów IP i reguły translacji adresów sieciowych są rdzennymi technologiami ochrony sieciowej, ale nie stanowią tego samego poziomu ochrony, co w pełni funkcjonalny produkt, jakim jest firewall. Należy bardzo starannie przeanalizować potrzeby i cele przed podjęciem decyzji o wyborze całkowitego produktu typu firewall lub funkcji reguł filtrowania pakietów w iSeries.

Wskazane jest zapoznanie się z tematem Wybów opcji ochrony iSeries na poziomie sieci, aby uzyskać pomoc w wyborze właściwego podejścia dla danej sieci.

Firewall

Firewall jest to blokada umieszczona na granicy między chronioną siecią wewnętrzną a siecią niezaufaną, jak Internet. W większości firm firewalli używa się do bezpiecznego przyłączenia sieci wewnętrznej do Internetu, chociaż firewall może także oddzielać jedną sieć wewnętrzną od drugiej.

Firewall pełni funkcję pilnie strzeżonych wrót między chronioną siecią wewnętrzną a siecią niezaufaną. Firewall:
- pozwala użytkownikom w obrębie sieci wewnętrznej korzystać ze z góry określonych zasobów znajdujących się w sieci zewnętrznej,
- uniemożliwia nieuprawnionym użytkownikom z sieci zewnętrznej korzystanie z zasobów sieci wewnętrznej.

Zastosowanie firewalla jako bramy do Internetu (lub innej sieci) zdecydowanie zwiększa bezpieczeństwo sieci wewnętrznej. W ten sposób uproszczona zostaje też administracja ochroną sieci, ponieważ firewall jest w stanie zrealizować wiele dyrektyw zapisanych w strategii ochrony.

Jak działa firewall

Aby zrozumieć sposób działania firewalla, należy wyobrazić sobie sieć jako budynek, do którego dostęp trzeba kontrolować. Jedynym wejściem jest hall. W hallu znajdują się: recepcjoniści, strażnicy ochrony, kamery wideo rejestrujące zachowanie gości oraz czytniki identyfikatorów sprawdzające tożsamość wchodzących do budynku osób.

Te środki zaradcze mogą dobrze funkcjonować, gdy chodzi o ochronę dostępu do budynku. Lecz jeśli osobie nie mającej uprawnień uda się dostać do wnętrza budynku, środki ochrony zastosowane w hallu przestają mieć znaczenie. Aby wykryć podejrzane zachowanie intruza, należałoby śledzić każdy jego krok w budynku.

Elementy składowe firewalla

Firewall składa się ze sprzętu i oprogramowania, które wspólnie zapobiegają nieautoryzowanemu dostępowi do części sieci. Elementy składowe firewalla to:
- Sprzęt. Sprzętowe składniki firewalla to zwykle osobny komputer lub inne urządzenie, którego wyłącznym zadaniem jest bycie jego platformą sprzętową.
- Oprogramowanie. Oprogramowanie firewalla to szereg różnych aplikacji. Od strony bezpieczeństwa sieci, firewall realizuje poniższe funkcje za pośrednictwem różnych technologii:
  - filtrowanie pakietów IP,
  - usługi translacji adresów sieciowych,
  - serwer SOCKS,
  - serwery proxy dla różnych usług, takich jak HTTP, Telnet, FTP itp.,
  - przekazywanie poczty,
  - rozdzielanie usługi DNS,
  - protokołowanie,
  - monitorowanie w czasie rzeczywistym.

Uwaga: Niektóre firewalle oferują także technologię sieci VPN, która pozwala zestawiać szyfrowane sesje między danym firewallem a innymi zgodnymi firewallami.

Korzystanie z funkcji firewalla

Aby zapewnić użytkownikom wewnętrznym bezpieczny dostęp do usług w Internecie, można użyć serwerów proxy lub SOCKS lub reguł translacji adresów sieciowych (NAT) firewalla. Serwery proxy i SOCKS przerywają połączenia TCP/IP na firewallu, aby ukryć dane z sieci wewnętrznej przed siecią niezaufaną. Serwery te udostępniają dodatkowe możliwości protokołowania.

Translacji adresu sieciowego (NAT) można użyć do zapewnienia użytkownikom Internetu łatwego dostępu do serwera publicznego za firewallem. Firewall nadal chroni sieć, ponieważ usługa NAT ukrywa wewnętrzne adresy IP.

Dodatkowa ochrona sieci wewnętrznej płynie z możliwości uruchomienia osobnego serwera DNS na potrzeby firewalla. Efektywnie działają wtedy dwa serwery DNS: jeden obsługujący żądania wyłącznie z sieci wewnętrznej i drugi, obsługujący żądania dotyczące zasobów sieci zewnętrznej, w tym żądania samego firewalla. Pozwala to ograniczyć dostęp z zewnątrz do informacji na temat systemów w sieci wewnętrznej.

Definiując strategię działania firewalla łatwo odnieść wrażenie, że wystarczy zabronić wszystkiego, co stanowi zagrożenie i dopuścić wszystko inne. Jednakże, ze względu na fakt, że przestępcy komputerowi ciągle wymyślają nowe metody ataku, należy być na to przygotowanym i przewidzieć sposoby zabezpieczenia. Nawiązując do przykładu z budynkiem, konieczne jest bezustanne monitorowanie wnętrza, by mieć pewność, że nikt nie zdołał ominąć wszystkich zabezpieczeń przy wejściu. Generalnie, bardziej kosztowne i pracochłonne jest naprawianie skutków włamań niż zapobieganie im.

W przypadku firewalla najlepszą strategią jest zezwolenie na działanie tylko tych aplikacji, które zostały wypróbowane i okazały się godne zaufania. Zgodnie z tym założeniem, konieczne jest zdefiniowanie wyczerpującej listy usług, które muszą być uruchomione w połączeniu z firewallem. Każda z usług charakteryzowana jest kierunkiem połączenia (z zewnątrz do wewnątrz lub z wewnątrz na zewnątrz). Należy ponadto zestawić listę użytkowników, którzy będą uprawnieni do korzystania z poszczególnych usług, jak również listę komputerów, z których mogą napływać żądania połączeń z daną usługą.

W jaki sposób firewall chroni sieć

Firewall instalowany jest w miejscu połączenia sieci wewnętrznej z Internetem (lub inną siecią niezaufaną). Firewall pozwala wtedy zdefiniować dozwolone punkty wejścia do sieci wewnętrznej. Firewall stanowi pojedynczy i jedyny punkt styku między siecią wewnętrzną a Internetem (patrz rysunek poniżej). Dysponowanie pojedynczym punktem styku pozwala zachować większą kontrolę nad dozwolonym przepływem danych do sieci i wypływem danych z sieci na zewnątrz.

Dla świata zewnętrznego firewall jest widziany jako pojedynczy adres. Udostępnia on zasoby sieci niezaufanych za pośrednictwem serwerów proxy lub SOCKS albo usługi translacji adresów sieciowych, ukrywając rzeczywiste adresy funkcjonujące w sieci wewnętrznej. Tym sposobem firewall strzeże poufności danych w sieci wewnętrznej. Ochrona poufności informacji na temat sieci wewnętrznej jest jedną z metod obrony przed atakiem przez podszycie się pod uprawnionego użytkownika (spoofing).

Firewall pozwala kontrolować przepływ informacji między siecią wewnętrzną a zewnętrzną w obie strony, minimalizując tym samym niebezpieczeństwo ataku. Firewall filtruje cały ruch przychodzący do sieci, dopuszczając tylko ściśle określone pakiety skierowane pod ściśle określone adresy. Pozwala to zmniejszyć ryzyko nieuprawnionego dostępu do systemów wewnętrznych za pośrednictwem takich usług, jak TELNET lub FTP.

Czego firewall nie może zapewnić

Firewall w znacznym stopniu uodparnia system na niektóre rodzaje ataków, lecz powinien być tylko jednym z elementów kompleksowego programu ochrony. Na przykład firewall nie zapewnia ochrony danych wysyłanych poprzez Internet w aplikacjach, takich jak poczta SMTP, usługi FTP lub sesje TELNET. Jeśli dane te nie zostaną przed wysłaniem poddane szyfrowaniu, osoba o złych intencjach może przechwycić je na drodze do miejsca przeznaczenia.

Reguły pakietów w iSeries

Reguły pakietów iSeries 400 to wbudowana funkcja systemu OS/400, dostępna za pośrednictwem interfejsu programu Operations Navigator. Pozwala ona na skonfigurowanie dwóch rdzennych technologii ochrony sieciowej w celu utrzymania kontroli nad ruchem pakietów TCP/IP i ochrony systemu iSeries:
- translacji adresu sieciowego (NAT),
- filtrowania pakietów IP.

Ponieważ NAT i filtrowanie pakietów IP są wbudowaną częścią systemu OS/400, stanowią ekonomiczną metodę chronienia systemu. W niektórych przypadkach te technologie ochrony mogą dostarczać wszystkiego co jest potrzebne, bez konieczności dodatkowych zakupów. Jednak nie utworzą one prawdziwego, funkcjonalnego firewalla. Można korzystać z samej ochrony pakietów lub w połączeniu z firewallem, w zależności od potrzeb i celów ochrony.

Uwaga: Przy planowaniu ochrony produkcyjnego systemu iSeries nie należy kierować się źle pojętą oszczędnością. W takich sytuacjach ochrona systemu powinna być ważniejsza niż koszty. Aby mieć pewność maksymalnego zabezpieczenia systemu produkcyjnego, należy użyć firewalla.

Co to jest NAT i filtrowanie pakietów IP i jak razem działają?

Translacja adresu sieciowego (NAT) polega na modyfikacji źródłowego lub docelowego adresu IP pakietów przesyłanych w systemie. Stanowi bardziej przezroczystą alternatywę serwerów proxy i SOCKS firewalla. Upraszcza także konfigurowanie sieci, umożliwiając łączenie sieci o niekompatybilnych strukturach adresowania. Używając reguł NAT, można korzystać z systemu iSeries jako bramy pomiędzy dwiema sieciami o niezgodnych schematach adresowania. Można także używać NAT do ukrywania prawdziwych adresów IP jednej sieci przez dynamiczne podstawianie jednego lub wielu adresów zamiast adresów prawdziwych. Ponieważ filtrowanie pakietów IP i NAT uzupełniają się wzajemnie, są często wspólnie używane w celu lepszej ochrony sieci.

Sterowanie publicznym serwerem WWW znajdującym się za firewallem jest znacznie prostsze przy korzystaniu z NAT. Publiczne adresy IP dla serwera WWW ulegają translacji na prywatne wewnętrzne adresy IP. Redukuje to liczbę zarejestrowanych adresów IP i minimalizuje wpływ na istniejącą sieć. Zapewnia to także dostęp do Internetu użytkownikom wewnętrznym, ukrywając prywatne wewnętrzne adresy IP.

Filtrowanie pakietów IP daje możliwość wybiórczego blokowania lub zabezpieczania ruchu IP w oparciu o informacje z nagłówków pakietów. Kreator konfiguracji internetowej w programie Operations Navigator pozwala w sposób szybki i prosty skonfigurować podstawowe reguły filtrowania w celu zablokowania niepożądanego ruchu pakietów w sieci.

Filtrowania pakietów IP można użyć do:
- Utworzenia zestawu reguł filtrowania w celu określenia, którym pakietom IP zezwolić na wejście do sieci, a którym zabronić dostępu. Tworząc reguły filtrowania, stosuje się je do interfejsu fizycznego (na przykład linii Token Ring lub Ethernet). Można stosować te same reguły do wielu interfejsów fizycznych lub stosować różne reguły do każdego interfejsu.
- Utworzenia reguł, które przyjmują lub odrzucają określone pakiety w oparciu o następujące informacje z nagłówka:
  - adres IP miejsca docelowego pakietu,
  - protokół adresu źródłowego IP (na przykład TCP, UDP itp.),
  - port docelowy (na przykład port 80 dla HTTP),
  - port źródłowy,
  - kierunek datagramu IP (przychodzący lub wychodzący),
  - przekazany lub lokalny.
- Ochrony aplikacji w systemie przed dostępem ze strony niepożądanego lub zbędnego ruchu w sieci. Można także zapobiegać przepływowi pakietów do innych systemów. Obejmuje to pakiety ICMP niskiego poziomu (na przykład pakiety PING), dla których nie jest wymagany żaden określony serwer aplikacji.

- Można określić, czy reguły filtrowania mają tworzyć w dzienniku systemowym pozycje zawierające informacje na temat pakietów i spełniania reguły. Gdy informacja zostaje zapisana jako pozycja dziennika systemowego, nie można już jej zmienić. Z tego powodu protokół jest idealnym narzędziem kontroli aktywności sieci.

Wybór opcji ochrony iSeries na poziomie sieci

Rozwiązania chroniące sieć przed dostępem użytkowników nie posiadających uprawnień oparte są z reguły na technologiach firewalla. Do ochrony systemu iSeries można wybrać w pełni funkcjonalny firewall lub wprowadzić wybrane technologie firewalla, będące częścią implementacji TCP/IP w OS/400. Implementacja obejmuje funkcję reguł pakietów (filtrowanie pakietów IP i translacja adresów sieciowych - NAT) oraz funkcję proxy serwera HTTP Server for iSeries.

Wybór między funkcją reguł pakietów a firewallem zależy od środowiska sieciowego, wymagań odnośnie dostępu i potrzeb ochrony. Podłączając system iSeries lub sieć wewnętrzną do Internetu, względnie do innej sieci niezaufanej, należy **poważnie** zastanowić się nad zastosowaniem firewalla jako głównej linii ochrony przed atakami.

Firewall jest w takiej sytuacji zabezpieczeniem najbardziej godnym polecenia, jako wyspecjalizowane urządzenie z odpowiednim oprogramowaniem i ograniczoną liczbą interfejsów do kontaktu z siecią zewnętrzną. Tymczasem technologie chronionego dostępu do Internetu w ramach implementacji TCP/IP w systemie OS/400 to platforma o niskim stopniu wyspecjalizowania i dająca wielką liczbę punktów połączenia między siecią zewnętrzną a wewnętrzną.

Ta różnica jest istotna z wielu względów. Na przykład, dedykowany produkt typu firewall nie realizuje żadnych funkcji ani aplikacji poza tymi, które wchodzą w skład samego firewalla. Jeśli więc atakującemu uda się nawet obejść firewall i zyskać dostęp do sieci, nie będzie mógł uczynić wiele złego. Jeśli natomiast atakujący ominie standardowe zabezpieczenia TCP/IP wbudowane w system iSeries, zyska tym samym potencjalny dostęp do wielu różnorodnych aplikacji, usług i danych. Nic nie powstrzyma go przed zniszczeniem tego systemu lub przed użyciem go w celu przedostania się do innych systemów w sieci.

Czy w takim razie ograniczenie się do standardowych zabezpieczeń TCP/IP w systemie iSeries jest kiedykolwiek uzasadnione? Podobnie jak w przypadku wszystkich decyzji dotyczących ochrony, należy rozważyć potencjalne korzyści przez porównanie z koniecznymi kosztami. Innymi słowy, trzeba przeanalizować priorytety związane z działaniem sieci i zastanowić się nad poziomem ryzyka, jaki jesteśmy w stanie zaakceptować i nad ceną, jaką jesteśmy gotowi zapłacić za minimalizowanie tego ryzyka. Poniższa tabela zawiera zestaw wskazówek pomocnych w podjęciu decyzji, kiedy można poprzestać na standardowych zabezpieczeniach TCP/IP, a kiedy należy użyć wyspecjalizowanego firewalla. Na podstawie tabeli łatwiej będzie ustalić, czy w danej sytuacji konieczny jest firewall, standardowe zabezpieczenia TCP/IP, czy też obie te techniki.

Technologia ochrony	Preferowane użycie zabezpieczeń OS/400 TCP/IP	Preferowane użycie dedykowanego firewalla
Filtrowanie pakietów IP	• Zapewnienie **dodatkowej** ochrony dla pojedynczego systemu iSeries, takiego jak publicznie dostępny serwer WWW lub system intranetowy z ważnymi danymi. • Ochrona podsieci w obrębie firmowego **intranetu**, kiedy system iSeries działa jako brama (router) na potrzeby pozostałej części sieci. • Kontrola nad komunikacją z częściowo zaufanym partnerem w ramach **sieci prywatnej** lub sieci zewnętrznej, przy czym system iSeries pełni funkcję bramy.	• Ochrona całej sieci firmowej od strony połączenia z **Internetem** lub z inną siecią niezaufaną. • Ochrona dużej podsieci, w której panuje nasilony przepływ pakietów, przed pozostałą częścią sieci firmy.

Technologia ochrony	Preferowane użycie zabezpieczeń OS/400 TCP/IP	Preferowane użycie dedykowanego firewalla
Translacja adresu sieciowego (NAT)	• Możliwość połączenia dwóch **sieci prywatnych** o niezgodnych strukturach adresowania. • Możliwość ukrycia adresów w podsieci przed mniej zaufaną siecią.	• Możliwość ukrycia adresów klientów korzystających z **Internetu** lub innej sieci niezaufanej. Alternatywa wobec serwerów Proxy i SOCKS. • Udostępnienie usług systemowych w sieci prywatnej klientom w sieci **Internet**.
Serwer proxy	• Pośredniczenie w połączeniach ze **zdalnymi miejscami** w sieci firmowej, w sytuacji gdy centralny firewall daje dostęp do Internetu.	• Pośredniczenie w połączeniach całej sieci firmowej z **Internetem**.

Więcej informacji na temat sposobu korzystania z funkcji zabezpieczających TCP/IP w OS/400 zawierają następujące dokumenty:

- Reguły pakietów (filtrowanie i translacja NAT).
- Centrum dokumentacji serwera HTTP. 
- Dokumentacja techniczna AS/400 Internet Security Scenarios: A Practical Approach  (SG24-5954).

Rozdział 7. Ochrona na poziomie aplikacji

Środki ochrony na poziomie aplikacji sterują interakcją użytkownika z określonymi aplikacjami. Należy skonfigurować ustawienia ochrony dla każdej używanej aplikacji. Szczególny nacisk należy położyć na ustawienie tych aplikacji, które będą używane lub dostarczane do Internetu. Takie aplikacje i usługi są narażone na nieprawidłowe użycie przez nieuprawnionych użytkowników szukających dostępu do systemów sieciowych. Wybrane środki ochrony powinny obejmować zagrożenie atakiem zarówno po stronie klienta, jak i serwera.

Jakkolwiek zabezpieczenie każdej używanej aplikacji ma duże znaczenie, środki ochrony na poziomie aplikacji są jedynie małym fragmentem kompleksowej strategii ochrony.

Więcej na temat ochrony niektórych powszechnie używanych aplikacji internetowych można znaleźć w sekcjach:

- “Serwer WWW - ochrona”
- “Język Java - ochrona” na stronie 24
- “Poczta elektroniczna - ochrona” na stronie 26
- “Protokół FTP - ochrona” na stronie 28

Serwer WWW - ochrona

Udostępniając serwis WWW, nie chcemy zazwyczaj, aby odwiedzający mieli wgląd w ustawienia serwera ani w kod użyty do wygenerowania strony. Strona powinna szybko się ładować i być łatwa i przyjemna w odbiorze, a kwestie techniczne powinny pozostać w ukryciu. Pełniąc funkcję administratora, należy upewnić się, że działania związane z ochroną nie wpłynęły negatywnie na atrakcyjność serwera WWW. Używając iSeries 400 w charakterze serwera WWW należy wziąć pod uwagę następujące czynniki:

- Administrator serwera musi zdefiniować dyrektywy dla serwera, zanim klient rozpocznie interakcję z serwerem HTTP. Tworzenie barier ochronnych może się odbywać dwiema metodami: poprzez ogólne dyrektywy serwera oraz poprzez dyrektywy ochronne serwera. Wszelkie żądania kierowane z sieci do serwera WWW muszą spełniać restrykcje nałożone tymi dyrektywami, aby serwer mógł na nie odpowiedzieć.
- Dyrektywy te można tworzyć i zmieniać używając stron WWW administratora serwera do konfigurowania serwera. Dyrektywy serwera pozwalają sterować ogólnym zachowaniem serwera WWW. Dyrektywy ochrony serwera pozwalają określić i sterować modelami ochrony używanymi przez serwer dla określonych adresów URL obsługiwanych przez serwer WWW.
- Konfigurując serwer można korzystać z dyrektyw MAP i PASS oraz stron administratora.
  - Aby zamaskować nazwy plików na serwerze WWW iSeries, należy użyć dyrektyw MAP lub PASS. Dyrektywy PASS i MAP nadzorują katalogi, z których serwer WWW obsługuje adresy URL. Istnieje także dyrektywa EXEC nadzorująca biblioteki, w których znajdują się programy CGI-BIN.

    Dla każdego adresu URL serwera można zdefiniować osobne dyrektywy ochrony. Nie wszystkie adresy URL wymagają dyrektyw ochrony. Jeśli trzeba sterować sposobem dostępu do adresu URL lub określać, kto może uzyskać dostęp, to wymagana jest dyrektywa ochrony adresu URL.
  - Konfigurując serwer, zamiast wpisywać dyrektywy i komendy Praca z Konfiguracją HTTP (Work with HTTP Configuration - WRKHTTPCFG), można używać stron administratora. Praca z dyrektywami ochrony wpisywanymi w wierszu komend może być bardzo skomplikowana. Dlatego też zaleca się korzystanie ze stron administratora, aby upewnić się, że dyrektywy zostały poprawnie wprowadzone.

Protokół HTTP dostarcza możliwości wyświetlenia danych, ale nie umożliwia zmiany danych w zbiorze bazy danych. Jednak istnieją aplikacje, które można napisać, gdy potrzebna jest aktualizacja zbioru bazy danych. W tym celu można użyć programów CGI-BIN. Na przykład, może zajść potrzeba tworzenia formularzy, które po wypełnieniu aktualizują bazę danych iSeries. Pełniąc funkcję administratora ochrony, należy monitorować uprawnienia profilu użytkownika i funkcje wykonywane przez programy CGI. Należy także sprawdzać, które chronione obiekty mogą mieć nieprawidłowe uprawnienia publiczne.

Uwaga: CGI (wspólny interfejs bramy) jest standardem służącym do wymiany informacji pomiędzy serwerem WWW i zewnętrznymi wobec niego programami komputerowymi. Programy te mogą być napisane w dowolnym języku programowania obsługiwanym przez system operacyjny, na którym działa serwer WWW.

Poza programami CGI na stronie WWW może zajść potrzeba używania języka Java. Przed dodaniem języka Java na strony WWW należy zapoznać się z sekcją Język Java - ochrona.

Serwer HTTP utrzymuje protokół dostępu, którego można używać do monitorowania zarówno pomyślnych, jak i niepomyślnych prób dostępu do serwera.

Serwer proxy otrzymuje żądania HTTP z przeglądarek WWW i wysyła je do serwerów WWW. Serwery WWW, które odbierają żądania, znają jedynie adres IP serwera proxy. Nie mogą ustalić nazw lub adresów komputerów osobistych, od których pochodzą żądania. Serwer proxy może obsługiwać żądania URL dla usług HTTP, FTP, Gopher i WAIS.

W celu skonsolidowania dostępu do usług WWW można też użyć obsługi serwera proxy HTTP w produkcie IBM HTTP Server for iSeries  . Serwer proxy może również protokołować wszystkie żądania URL do celów śledzenia. Protokołów można używać do monitorowania właściwego i niewłaściwego użytkowania zasobów sieciowych.

Więcej informacji na ten temat można znaleźć w książce *Wskazówki i narzędzia dotyczące ochrony iSeries*. 

Język Java - ochrona

We współczesnych zastosowaniach komputerów coraz większą popularność zyskują programy napisane w języku Java. Przykładami pakietów służących do programowania w tym języku są IBM Toolbox for Java lub IBM Development Kit for Java. Dlatego też należy przygotować się na rozwiązywanie problemów ochrony związanych z językiem Java. Jakkolwiek firewall zapewnia dobrą ochronę przed większością zagrożeń ze strony sieci Internet, nie zabezpiecza ona przed wieloma zagrożeniami związanymi z językiem Java. Strategia ochrony powinna szczegółowo określać zasady zabezpieczenia systemu od strony trzech sposobów zastosowania języka Java: aplikacji, apletów i serwletów. Ponadto wymagane jest dobre zrozumienie zasad interakcji między funkcjami ochrony zasobów a autoryzacją i uwierzytelnianiem programów w języku Java.

Aplikacje w języku Java

Jako język, Java ma kilka cech charakterystycznych, które chronią programistów przed popełnieniem nieumyślnych błędów, powodujących problemy z integralnością. (Inne języki powszechnie używane do tworzenia aplikacji dla komputerów osobistych, takie jak C lub C++, nie chronią programistów przed nieumyślnymi błędami w takim stopniu, jak Java). Na przykład język Java korzysta z mechanizmów silnej typizacji, które chronią programistę przed używaniem obiektów w niezamierzony sposób. Język Java nie pozwala na manipulację wskaźnikami, co chroni programistę przed przypadkowym dostępem poza pamięć przeznaczoną dla programu. Z perspektywy tworzenia aplikacji język Java można więc traktować jak inne języki programowania wysokiego poziomu. Należy stosować te same reguły ochrony dla tworzenia aplikacji jak w przypadku innych języków programowania w iSeries 400.

Aplety w języku Java

Aplety w języku Java to małe programy, które można umieścić na stronach HTML. Aplety uruchamiane są na komputerze klienta, stanowią więc dla niego problem. Niemniej jednak aplet języka Java ma możliwość dostępu do systemu iSeries 400. (Na podobnej zasadzie, dostęp do systemu iSeries może uzyskać program korzystający z interfejsu ODBC lub pracujący w standardzie APPC (zaawansowana komunikacja program-program), uruchomiony na dowolnym komputerze osobistym w sieci). Ogólnie aplet w języku Java

może nawiązać sesję tylko z serwerem, z którego pochodzi. Dlatego też aplet języka Java może uzyskać dostęp do serwera iSeries z podłączonego komputera osobistego tylko, gdy pochodzi z tego serwera (na przykład z serwera WWW).

Aplet może próbować podłączyć się do dowolnego portu TCP/IP serwera. Nie musi komunikować się z serwerem oprogramowania napisanym w języku Java. Jednak w przypadku serwerów napisanych za pomocą biblioteki IBM Toolbox for Java aplet musi dostarczyć identyfikator użytkownika i hasło podczas nawiązywania połączenia z serwerem. Wszystkie serwery opisywane w tej dokumentacji są serwerami iSeries. (Serwer napisany w języku Java nie musi korzystać z biblioteki IBM Toolbox for Java). Zwykle klasa IBM Toolbox for Java przy pierwszym połączeniu prosi użytkownika o identyfikator i hasło.

Aplet może wykonywać funkcje w systemie iSeries tylko wtedy, gdy profil użytkownika ma uprawnienia do tych funkcji. Dlatego też dobry schemat ochrony zasobów jest bardzo ważny zwłaszcza na początku stosowania apletów w języku Java w celu zapewnienia nowych funkcji aplikacji. Gdy system przetwarza żądania z apletów, nie korzysta z kontroli dostępu poprzez menu ani z wartości ograniczonej funkcjonalności w profilu użytkownika.

AppletViewer pozwala testować aplet w systemie serwera; nie podlega on jednak ograniczeniom ochrony przeglądarki. Dlatego też należy korzystać z programu AppletViewer tylko do testowania, nigdy zaś do uruchamiania apletów pochodzących z zewnątrz. Aplety w języku Java często zapisują dane na napędzie komputera osobistego użytkownika, co może dać apletowi okazję do destrukcyjnego działania. Jednak tożsamość apletu w języku Java można określić, podpisując go za pomocą certyfikatu cyfrowego. Podpisany aplet może zapisywać na lokalnym napędzie komputera osobistego, nawet jeśli domyślne ustawienia przeglądarki zabraniają tego. Podpisany aplet może także pisać na odwzorowanych dyskach iSeries, ponieważ komputer osobisty traktuje je jak napędy lokalne.

Uwaga: Opisany sposób działania na ogół sprawdza się dla przeglądarek Netscape Navigator i MS Internet Explorer. To, co się zdarzy w rzeczywistości, zależy w dużej mierze od sposobu konfiguracji i zarządzania używanymi przeglądarkami.

W przypadku własnych apletów w języku Java, dołączonych do iSeries, może być wskazane korzystanie z podpisów cyfrowych. Należy jednak pouczyć użytkowników, aby nie akceptowali podpisanych apletów z nieznanego źródła.

Już od wersji V4R4 możliwe jest korzystanie z pakietu IBM Toolbox for Java w celu skonfigurowania protokołu SSL (Secure Sockets Layer). Zabezpieczanie aplikacji w Języku Java za pomocą SSL możliwe jest też za pomocą pakietu IBM Developer Toolkit for Java. Zastosowanie protokołu SSL polega na szyfrowaniu danych przesyłanych między klientem a serwerem, takich jak identyfikator i hasło użytkownika. W celu skonfigurowania zarejestrowanych programów w języku Java na potrzeby protokołu SSL można się posłużyć programem Digital Certificate Manager.

Serwlety w języku Java

Serwlety to komponenty serwera napisane w języku Java, które dynamicznie rozszerzają funkcjonalność serwera WWW nie zmieniając kodu serwera. IBM WebSphere Application Server dołączony do IBM HTTP Server for iSeries zapewnia obsługę serwletów w systemach iSeries.

Należy korzystać z ochrony zasobów wobec obiektów, z których korzysta serwer. Jednak zastosowanie do serwleta ochrony zasobów nie wystarczy do jego ochrony. Gdy serwer WWW załaduje serwlet, ochrona zasobów nie zapobiegnie uruchomieniu go przez innych użytkowników. Dlatego funkcji ochrony zasobów należy używać w połączeniu z funkcjami i dyrektywami ochrony serwera HTTP. Na przykład, nie należy zezwalać serwletom na działanie wyłącznie w profilu serwera WWW. Ponadto należy określić, komu wolno uruchamiać serwlet (słowa kluczowe mask w dyrektywie ochrony). Służą do tego grupy i listy kontroli dostępu serwera HTTP. Niezależnie od tego, należy korzystać z funkcji ochronnych zapewnianych przez pakiet użyty do utworzenia serwleta, na przykład WebSphere Application Server for iSeries.

Aby dowiedzieć się więcej na temat działań zwiększających ogólny poziom bezpieczeństwa od strony języka Java, można skorzystać z poniższych dokumentów:
- IBM Developer Kit for Java Java Security.
- IBM Toolbox for Java security classes.
- Wskazówki i narzędzia dotyczące ochrony iSeries  .

Uwierzytelnianie i autoryzacja dostępu programów w języku Java do zasobów

Produkt IBM Toolbox for Java zawiera klasy ochrony umożliwiające weryfikację tożsamości użytkownika i ewentualne przypisanie tej tożsamości wątkowi systemu operacyjnego dla aplikacji lub serwleta działającego w systemie iSeries. Następnie sprawdzanie ochrony zasobów będzie się odbywało dla przypisanej tożsamości. Więcej informacji na temat klas funkcji ochronnych można znaleźć w dokumencie IBM Toolbox for Java Authentication Services.

Pakiet IBM Developer Kit for Java zapewnia obsługę usług uwierzytelniania i autoryzacji dla języka Java (JAAS), które są standardem rozszerzającym funkcjonalność standardowej edycji Java 2 Software Development Kit (J2SDK). Obecnie J2SDK obejmuje funkcje kontroli dostępu bazujące na pochodzeniu kodu i na jego podpisie. Więcej informacji na temat korzystania z J2SDK można znaleźć w sekcji Java Authentication and Authorization Service.

Ochrona aplikacji w języku Java za pomocą protokołu SSL

Aby chronić komunikację aplikacji systemu iSeries, można skorzystać z protokołu SSL, dostarczanego wraz z pakietem IBM Developer Kit for Java. Aplikacje typu klient korzystające z IBM Toolbox for Java także mogą korzystać z zalet SSL. Proces udostępniania protokołu SSL własnym aplikacjom różni się znacznie od udostępniania tego protokołu innym aplikacjom.

Więcej informacji na temat administrowania protokołem SSL na potrzeby aplikacji w języku Java można znaleźć w następujących tematach Centrum informacyjnego:
- IBM Toolbox for Java Secure Sockets Layer (SSL) environment.
- IBM Developer Toolkit for Java to make a Java application secure with SSL.

Poczta elektroniczna - ochrona

Korzystanie z poczty elektronicznej w sieci Internet lub innej sieci niezaufanej powoduje zagrożenia, przed którymi nie chroni firewall. Należy koniecznie zrozumieć istotę tych zagrożeń, aby upewnić się, że w strategii ochrony opisano sposoby ich minimalizacji.

Poczta elektroniczna nie różni się od innych form komunikacji. Przed wysłaniem poufnych informacji pocztą elektroniczną bardzo ważne jest zapewnienie dyskrecji. Ponieważ wiadomość pocztowa, zanim dotrze do celu, musi przejść przez wiele serwerów, możliwe jest jej przechwycenie i odczytanie. Dlatego celowe jest podjęcie kroków zmierzających do odpowiedniego zabezpieczenia wiadomości poczty elektronicznej.

Powszechne zagrożenia związane z pocztą elektroniczną

Istnieją pewne zagrożenia powiązane z korzystaniem z poczty elektronicznej:
- **Zalanie (flooding)** (atak typu odmowa usługi) polega na zalaniu systemu olbrzymią ilością poczty elektronicznej. Stosunkowo proste jest utworzenie programu generującego i wysyłającego miliony wiadomości pocztowych (nawet pustych) na wybrany serwer w celu jego przepełnienia i unieruchomienia. W przypadku braku odpowiednich zabezpieczeń serwer będący celem ataku może zostać zablokowany, ponieważ jego dysk zostanie zapełniony bezużytecznymi wiadomościami. Innym powodem, dla którego serwer może przestać reagować na wywołania, jest zaangażowanie wszystkich jego zasobów w przetwarzanie poczty wysłanej w złej wierze.
- **Zapchanie (spam)** (poczta elektroniczna zawierająca śmieci - junk e-mail) to inny popularny typ ataku na pocztę elektroniczną. Przy rosnącej liczbie firm prowadzących działalność handlową w sieci Internet,

można zaobserwować eksplozję niechcianej, wysyłanej bez żądania poczty powiązanej z tymi firmami. Są to pocztowe śmieci, wysyłane do dużych list dystrybucyjnych użytkowników poczty elektronicznej, wypełniające skrzynki wszystkich użytkowników.
- **Poufność** jest zagrożeniem związanym z wysłaniem poczty elektronicznej do innej osoby za pośrednictwem Internetu. Taki e-mail, zanim dotrze do adresata, przejdzie przez wiele serwerów. Jeśli wiadomość nie została zaszyfrowana, haker może wydostać i odczytać pocztę w dowolnym miejscu wzdłuż trasy dostarczania.

Opcje ochrony poczty elektronicznej

Aby zabezpieczyć się przed zalewem wiadomości oraz otrzymywaniem niepożądanych przesyłek, należy odpowiednio skonfigurować serwer poczty elektronicznej. Większość aplikacji serwerowych daje możliwość ochrony przed tego rodzaju atakami. Ponadto, celem zapewnienia sobie dodatkowej ochrony, można nawiązać współpracę z dostawcą usług internetowych.

Ewentualna konieczność zastosowania dodatkowych środków zabezpieczających zależy od żądanego poziomu poufności danych, jak również od funkcji ochronnych oferowanych przez posiadane aplikacje obsługi poczty. Na przykład, czy wystarczy ochrona poufności treści listu elektronicznego? Czy konieczne jest zachowanie w ukryciu wszystkich informacji związanych z wiadomością elektroniczną, takich jak źródłowy i docelowy adres IP?

Niektóre aplikacje mają wbudowane opcje, które mogą zapewnić wymaganą ochronę. Na przykład Lotus Notes Domino ma kilka zintegrowanych funkcji ochronnych, takich jak możliwość szyfrowania całego dokumentu lub wybranych pól w dokumencie.

W celu zaszyfrowania poczty Lotus Notes Domino tworzy unikalny klucz publiczny i klucz prywatny dla każdego użytkownika. Wiadomość szyfrowana jest za pomocą klucza prywatnego użytkownika, a więc odczytać ją mogą tylko użytkownicy dysponujący odpowiednim kluczem publicznym. Aby adresat mógł odczytać list, klucz publiczny musi zostać uprzednio przekazany odbiorcy wiadomości. Po otrzymaniu zaszyfrowanej poczty Lotus Notes Domino użyje klucza publicznego nadawcy do odszyfrowania wiadomości.

Informacje na temat korzystania z funkcji szyfrowania w Lotus Notes można znaleźć w plikach pomocy ekranowej tego programu.

Dodatkowe informacje na temat zabezpieczeń wbudowanych w Domino w systemie iSeries można znaleźć w poniższych materiałach:

- Biblioteka referencji Lotus Domino. 
- Internetowy serwis pomocy technicznej Lotus Notes. 
- Lotus Notes and Domino R5.0 Security Infrastructure Revealed  (SG24-5341).
- Lotus Domino for AS/400 Internet Mail and More  (SG24-5990).

Kiedy zachodzi potrzeba zapewnienia wyższego poziomu poufności dla poczty lub innych danych wymienianych z innym oddziałem firmy, ze zdalnie połączonym użytkownikiem lub z partnerem handlowym, do wyboru jest kilka opcji.

Jeśli aplikacja serwera poczty elektronicznej obsługuje protokół SSL, funkcji tej można użyć do zestawiania chronionych sesji komunikacyjnych między serwerem a klientami poczty. SSL oferuje ponadto możliwość opcjonalnego uwierzytelniania klienta, pod warunkiem że możliwość taką przewidziano także w aplikacji klienta. Ponieważ cała sesja jest szyfrowana, SSL zapewnia przy okazji integralność danych w trakcie ich przesyłania.

Inną opcją jest skonfigurowanie połączenia w ramach sieci VPN. Poczynając od wersji V4R4 serwer iSeries pozwala na konfigurowanie rozmaitych połączeń VPN, także z udziałem klientów zdalnych. Przy korzystaniu z sieci VPN wszystkie dane przesyłane między dwoma punktami końcowymi są szyfrowanie, co gwarantuje zarówno poufność, jak i integralność danych.

Protokół FTP - ochrona

Protokół FTP umożliwia przesyłanie plików pomiędzy klientem (użytkownikiem w jednym systemie) a serwerem. Można także korzystać z funkcji zdalnego wykonywania komend, aby przekazywać komendy do systemu serwera. Dlatego też protokół FTP jest bardzo przydatny przy pracy ze zdalnymi systemami lub przy przenoszeniu plików pomiędzy systemami. Jednak korzystanie z FTP w sieci Internet lub w innych sieciach niezaufanych wiąże się z pewnymi zagrożeniami. Zagrożenia te należy dobrze sobie uświadomić, aby mieć pewność, że strategia ochrony przewiduje sposoby ich minimalizowania.

- Schemat uprawnień do obiektów może nie zapewniać wystarczającej ochrony, gdy w systemie działa FTP.

  Na przykład uprawnienia publiczne do obiektów mogą mieć wartość *USE, a dostępowi do nich większości użytkowników zapobiega się korzystając z ″ochrony poprzez menu″. (Ochrona poprzez menu zapobiega wykonywaniu przez użytkowników czynności nie będących jedną z opcji ich menu). Użytkowników FTP nie obejmują ograniczenia dotyczące menu i dlatego mogą odczytywać wszystkie obiekty w systemie.Poniżej przedstawiono kilka możliwości zapobiegania takim zagrożeniom:
  - Uaktywnij pełną ochronę obiektów iSeries w systemie (innymi słowy, zmień model ochrony z ″ochrony poprzez menu″ na ″ochrona obiektów″). To jest najlepsza, najbardziej bezpieczna opcja.
  - Napisz program obsługi wyjścia dla protokołu FTP, aby ograniczyć dostęp do plików, które mogą być przekazywane przez FTP. Programy obsługi wyjścia powinny zapewniać ochronę przynajmniej na poziomie oferowanym przez programy menu. Wielu klientów będzie prawdopodobnie chciała wprowadzić jeszcze bardziej restrykcyjną kontrolę dostępu przez FTP. Opcja ta obejmuje tylko protokół FTP, a nie inne interfejsy, takie jak ODBC, DDM czy DRDA.

    Uwaga: Uprawnienie *USE do pliku pozwala użytkownikowi pobrać dany plik. Uprawnienie *CHANGE pozwala użytkownikowi przesłać dany plik.
- Haker może wykorzystać protokół FTP do przeprowadzenia na serwer ataku typu ″odmowa usługi″ i zablokowania profili użytkowników w systemie. Atak tego typu polega na wielokrotnie powtarzanych próbach zalogowania się w profilu użytkownika za pomocą błędnego hasła, aż profil zostanie zablokowany. Zablokowanie profilu następuje po tym, jak liczba nieudanych prób logowania osiągnie wartość maksymalną, równą trzy.

  Zmniejszenie ryzyka ataku wymaga pójścia na pewne kompromisy. Dążenie do zwiększenia poziomu bezpieczeństwa systemu zwykle wiąże się z utrudnieniami w dostępie dla zwykłych użytkowników. Serwer FTP zazwyczaj wymusza ograniczanie wartości parametru QMAXSIGN, aby odebrać hakerom możliwość wykonywania wielokrotnych prób logowania, gdyż mogłoby to się skończyć odgadnięciem przez nich hasła. Oto kilka sposobów postępowania, które warto rozważyć:
  - Użycie programu obsługi wyjścia logowania się do serwera FTP, aby odrzucić żądania zalogowania profili użytkowników systemowych oraz profili użytkowników, którym wprost odebrano prawo dostępu do FTP. (Przy korzystaniu z takiego programu obsługi wyjścia, próby zalogowania dla profilu bez prawa dostępu, odrzucone przez punkt wyjścia logowania się do serwera FTP, **nie** są zliczane w limicie prób logowania QMAXSIGN).
  - Użycie programu obsługi wyjścia w celu wskazania określonych komputerów, z których dany profil użytkownika może łączyć się z serwerem FTP. Na przykład, jeśli osoba z działu księgowości ma dostęp do FTP, należy zezwolić temu profilowi użytkownika na dostęp do serwera FTP tylko z komputerów o adresach IP z zakresu przydzielonego działowi księgowości.
  - Użycie programu obsługi wyjścia logowania do zapisywania nazwy użytkownika i adresu IP wszystkich prób zalogowania się do usługi FTP. Protokoły te należy przeglądać regularnie i jeśli profil użytkownika został zablokowany przez maksymalną liczbę prób hasła, należy za pomocą informacji o adresie IP zidentyfikować napastnika i podjąć odpowiednie środki.

Dodatkowo, punkty wyjścia serwera FTP można wykorzystać w celu zapewnienia dostępu użytkownikom anonimowym. Skonfigurowanie chronionego anonimowego serwera FTP wymaga programów obsługi wyjścia dla punktów wyjścia logowania do serwera FTP **oraz** sprawdzania poprawności żądania serwera FTP.

Poczynając od wersji V5R1 sesje komunikacyjne z serwerem FTP mogą być chronione za pomocą protokołu SSL. Protokół SSL umożliwia szyfrowanie wszystkich danych przesyłanych w ramach sesji FTP, co zapewnia poufność między innymi nazwy i hasła użytkownika. Ponadto serwer FTP może korzystać z certyfikatów cyfrowych w celu uwierzytelniania klienta.

Więcej informacji na temat korzystania z FTP, związanych z tym zagrożeń i dostępnych środków bezpieczeństwa można znaleźć w poniższych dokumentach:
- Implementing FTP security.
- Anonymous FTP.
- Securing FTP.
- Wskazówki i narzędzia dotyczące ochrony iSeries  .

Rozdział 8. Opcje ochrony transmisji

Przypomnijmy, że scenariusz dla firmy JKL Toy obejmował dwa podstawowe systemy iSeries 400. Jeden wykorzystywany dla potrzeb projektowania, a drugi do zastosowań produkcyjnych. Oba systemy obsługują dane i aplikacje o znaczeniu krytycznym. Dlatego też firma zdecydowała się na dodanie nowego systemu iSeries w sieci obwodowej, który służyć będzie do celów związanych z działaniem intranetu i dostępem do Internetu.

Ustanowienie sieci obwodowej daje pewność, że istnieje fizyczna separacja pomiędzy siecią wewnętrzną a Internetem. Separacja ta zmniejsza niebezpieczeństwo ze strony sieci Internet, na które narażone są systemy wewnętrzne. Przeznaczenie nowego systemu iSeries 400 tylko do obsługi Internetu pozwala ponadto uprościć zarządzanie ochroną sieci.

Potrzeby ochrony w środowisku Internetu powodują, że firma IBM dostarcza ciągle nowych ofert ochrony, aby zapewnić bezpieczne środowisko sieciowe dla biznesu elektronicznego w Internecie. W przypadku sieci mającej podłączenie do Internetu konieczne jest wdrożenie odpowiedniej ochrony zarówno z punktu widzenia systemu, jak i z punktu widzenia aplikacji. Przesyłanie danych poufnych w obrębie firmowej sieci intranet, czy też przez połączenie z Internetem, zwiększa potrzebę zastosowania silniejszych zabezpieczeń. Aby uniknąć zagrożeń, należy użyć funkcji zapewniających ochronę danych przesyłanych za pośrednictwem Internetu.

Zagrożenia związane z przesyłaniem informacji poprzez niezaufane systemy można zminimalizować za pomocą dwóch funkcji systemu iSeries, przeznaczonych specjalnie do ochrony danych na poziomie transmisji: chronionej komunikacji z użyciem protokołu SSL i połączeń siecią VPN.

Ochrona aplikacji za pomocą protokołu SSL

Protokół Secure Sockets Layer (SSL) jest obecnie standardem chronionej komunikacji pomiędzy klientem a serwerem. Protokół SSL pierwotnie był przeznaczony dla aplikacji przeglądarek WWW, ale liczba innych aplikacji korzystających z tego protokołu wciąż wzrasta. W przypadku systemu iSeries są to:

- IBM HTTP Server for iSeries (oryginalny, jak i oparty na serwerze Apache),
- serwer FTP,
- serwer Telnet,
- architektura rozproszonej relacyjnej bazy danych (DRDA) i zarządzanie danymi rozproszonymi,
- serwer (DDM),
- Centrum Zarządzania,
- serwer usług katalogowych (LDAP),
- aplikacje Client Access Express, w tym Operations Navigator, jak również aplikacje napisane z użyciem zestawu interfejsów programistycznych (API) programu Client Access Express,
- programy opracowane za pomocą pakietu Developer Kit for Java oraz aplikacje klienckie korzystające z klas IBM Toolkit for Java,
- programy opracowane z użyciem interfejsów programistycznych SSL, które mogą służyć do włączania obsługi protokołu SSL przez aplikacje. Więcej informacji dotyczących tworzenia aplikacji korzystających z protokołu SSL można znaleźć w temacie Secure Sockets Layer APIs.

Niektóre z tych aplikacji obsługują także uwierzytelnianie klienta za pośrednictwem certyfikatów cyfrowych. Protokół SSL polega na certyfikatach cyfrowych podczas uwierzytelniania stron komunikacji i podczas tworzenia chronionego połączenia.

Sieci VPN systemu iSeries

Systemu iSeries można użyć do ustanowienia chronionego kanału komunikacyjnego za pomocą połączenia VPN pomiędzy dwoma punktami końcowymi. Podobnie jak w przypadku połączenia SSL dane przemieszczające się pomiędzy dwoma punktami końcowymi mogą być szyfrowane, co gwarantuje ich poufność i integralność. Połączenia VPN pozwalają ograniczyć przepływ ruchu do podanych punktów

końcowych i ograniczyć typy pakietów, których można używać w połączeniu. Dlatego też połączenia VPN dostarczają pewnego poziomu ochrony sieciowej pomagając zabezpieczyć zasoby sieciowe przed niepowołanym dostępem.

Której metody użyć?

Obie metody ochrony mają w założeniu zapewnić bezpieczeństwo uwierzytelniania oraz poufność i integralność danych. Wybór jednej z nich zależy od kilku czynników. Należy rozważyć takie okoliczności, jak to, z kim nawiązywana jest komunikacja, za pomocą jakich aplikacji, w jakim stopniu sesja komunikacyjna ma być zabezpieczona i jakie ustępstwa pod względem kosztów i wydajności można ponieść w celu zapewnienia ochrony komunikacji.

Ponadto, aplikacje mające współpracować z protokołem SSL muszą zostać specjalnie skonfigurowane pod tym kątem. Wiele aplikacji jeszcze nie potrafi korzystać z protokołu SSL. Inne, takie jak Telnet czy Client Access Express, zostały uzupełnione o taką możliwość. Sieci VPN natomiast pozwalają na zabezpieczenie całego ruchu pakietów IP, przepływającego pomiędzy określonymi punktami końcowymi.

Na przykład, w obecnej konfiguracji sieci partnerzy handlowi mogą korzystać z zasobów wewnętrznej sieci firmy za pośrednictwem serwera HTTP w sesjach chronionych protokołem SSL. Jeśli serwer WWW jest jedyną aplikacją, która wymaga ochrony podczas komunikacji między siecią wewnętrzną a partnerem handlowym, przechodzenie na technikę VPN może nie być potrzebne. Jeśli jednak zakres form komunikacji będzie poszerzany, połączenie VPN może mieć rację bytu. Może zaistnieć również sytuacja, w której wymagane jest zabezpieczenie ruchu we fragmencie sieci, a chcemy uniknąć konfigurowania każdego klienta i serwera do korzystania z SSL. Należy wtedy utworzyć połączenie VPN między bramkami dla tej części sieci. Rozwiązanie takie pozwala chronić ruch, pozostając niezauważalne dla serwerów i klientów po obu stronach połączenia.

Korzystanie z certyfikatów cyfrowych w połączeniu z protokołem SSL

Certyfikaty cyfrowe stanowią podstawę do korzystania z protokołu SSL dla komunikacji chronionej i są dobrą metodą uwierzytelniania. System iSeries 400 daje możliwość łatwego tworzenia i zarządzania certyfikatami cyfrowymi dla systemu i użytkowników za pomocą programu Digital Certificate Manager (DCM), wbudowanej opcji OS/400.

Ponadto istnieje możliwość skonfigurowania niektórych aplikacji, takich jak IBM HTTP Server for iSeries, aby korzystały z certyfikatów cyfrowych w celu zapewnienia lepszych metod uwierzytelniania klientów, niż nazwy i hasła użytkownika.

Co to jest certyfikat cyfrowy?

Certyfikat cyfrowy jest to dokument elektroniczny, który potwierdza tożsamość właściciela certyfikatu w podobny sposób jak paszport. Zaufana strona pośrednicząca, nazywana **Ośrodkiem certyfikacji (CA),** wystawia certyfikaty cyfrowe dla użytkowników i serwerów. Zaufanie do ośrodka certyfikacji stanowi fundament zaufania do certyfikatu jako dokumentu uwierzytelniającego.

Każdy ośrodek certyfikacji ma własną strategię określającą, jakie dane identyfikacyjne są konieczne do wystawienia certyfikatu. Niektóre spośród ośrodków certyfikacji wymagają niewielu informacji, jak na przykład tylko nazwy wyróżniającej. Nazwa wyróżniająca jest nazwą osoby lub serwera, dla którego ośrodek certyfikacji ma wydać adres certyfikatu cyfrowego i adres poczty elektronicznej. Dla każdego certyfikatu jest generowany klucz prywatny i publiczny. Certyfikat zawiera klucz publiczny, a przeglądarka lub plik chroniony przechowuje klucz prywatny. Właściciel certyfikatu może korzystać z tych kluczy do ″podpisywania″ i szyfrowania danych, takich jak komunikaty i dokumenty wysyłane pomiędzy użytkownikami i serwerami. Podpisy cyfrowe zapewniają wiarygodność źródła i chronią integralność danych.

Wiele aplikacji jeszcze nie potrafi korzystać z protokołu SSL. Inne, takie jak Telnet czy Client Access Express, zostały uzupełnione o taką możliwość. Informacje o sposobie korzystania z protokołu SSL w połączeniu z aplikacjami iSeries można znaleźć w temacie Centrum informacyjnego iSeries **Ochrona aplikacji za pomocą SSL**.

Protokół SSL dla chronionego dostępu poprzez Telnet

W wersji V4R4 możliwe jest takie skonfigurowanie serwera Telnet, aby umożliwić ochronę sesji komunikacyjnych Telnet za pomocą protokołu SSL. Pierwszym krokiem podczas konfigurowania serwera Telnet na potrzeby protokołu SSL jest użycie programu Menedżer certyfikatów cyfrowych (Digital Certificate Manager - DCM) w celu utworzenia certyfikatu serwera. Domyślnie serwer Telnet obsługuje zarówno połączenia chronione, jak i niechronione. Można jednak skonfigurować usługę Telnet tak, aby dozwolone były tylko sesje chronione. Ponadto serwer Telnet może wymagać dodatkowego uwierzytelniania klientów przez żądanie od nich cyfrowych certyfikatów.

Ochrona sesji Telnet przez SSL daje wiele korzyści z punktu widzenia bezpieczeństwa systemu. Dla usługi Telnet, oprócz uwierzytelniania serwera, dane są szyfrowane, zanim przepłyną jakiekolwiek dane protokołu Telnet. Gdy ustanowiona jest sesja SSL, wszystkie dane protokołu Telnet, łącznie z identyfikatorem użytkownika i wymianą haseł, są szyfrowane.

Najważniejszym czynnikiem do rozważania przy stosowaniu serwera Telnet jest ważność informacji używanych w sesji klienta. Zastosowanie protokołu SSL jest szczególnie wskazane, jeśli przesyłane dane są cenne lub poufne. Po utworzeniu certyfikatu cyfrowego dla aplikacji Telnet serwer Telnet jest w stanie obsługiwać sesje klientów zarówno z użyciem protokołu SSL, jak i bez niego. Jeśli strategia ochrony wymaga, aby sesje Telnet zawsze były szyfrowane, można zablokować wszystkie sesje Telnet, które nie używają SSL. Jeśli nie ma potrzeby użycia serwera Telnet obsługującego SSL, można wyłączyć port SSL. Port można zablokować komendą ADDTCPPORT. Po wyłączeniu portu serwer udostępnia klientom usługę Telnet bez obsługi SSL, a sesje Telnet obsługujące SSL zostają wyłączone.

Więcej informacji na temat usługi Telnet i wskazówek dotyczących jej ochrony (z wykorzystaniem warstwy SSL i bez niej) można znaleźć w poniższych materiałach:

- Temat Telnet w Centrum informacyjnym zawiera informacje wymagane przy korzystaniu z usługi Telnet na serwerze iSeries.
- Temat Ochrona sesji Telnet zawiera informacje dotyczące zabezpieczania sesji komunikacyjnych Telnet z użyciem protokołu SSL.
- Temat Wskazówki i narzędzia dotyczące ochrony iSeries  w sekcji poświęconej protokołowi TCP/IP zawiera szczegółowe informacje na temat bezpieczeństwa usługi Telnet.

Protokół SSL dla chronionego programu Client Access Express

W wersji V4R4 możliwe jest takie skonfigurowanie serwera Client Access Express, aby umożliwić zabezpieczanie sesji komunikacyjnych za pomocą protokołu SSL. Na przykład, gdy firma JKL Toy się rozrosła, personel uzupełniony został o pewną liczbę pracujących w terenie przedstawicieli handlowych. Potrzebują oni dostępu do informacji z produkcyjnego serwera iSeries, aby sprawdzić, czy dana zabawka jest dostępna oraz jakie są terminy zakończenia produkcji. Ponieważ dane te należą do poufnych, firma JKL Toy umożliwiła dostęp do nich wyłącznie w ramach chronionej sesji połączeniowej Client Access Express.

Używanie protokołu SSL zapewnia, że wszystkie pakiety sesji Client Access Express są szyfrowane. Dzięki temu dane nie są czytelne w momencie przekazywania ich pomiędzy lokalnym i zdalnym hostem.

Więcej informacji na temat korzystania z protokołu SSL w połączeniu z Client Access Express można znaleźć w poniższych dokumentach:

- Secure Sockets Layer Administration
- Securing Client Access Express and Operations Navigator
- IBM Developer Kit for Java SSL

- IBM Java Toolbox SSL

Sieć VPN dla chronionej prywatnej komunikacji

Kierując się wzrostem popularności techniki wirtualnych sieci prywatnych (VPN) oraz wysokim poziomem zapewnianego przez nie bezpieczeństwa, w firmie JKL Toy poważnie rozważane jest wdrożenie takiej sieci w celu przesyłania danych przez Internet. Firma ta wykupiła niedawno inną małą firmę wytwarzającą zabawki i zamierza z nią współdziałać. Konieczne jest utworzenie kanału wymiany informacji między dwiema firmami. Obie firmy posiadają systemy iSeries, a sieć VPN zapewnia należytą ochronę danych przesyłanych przy komunikacji między nimi. Utworzenie sieci VPN jest rozwiązaniem tańszym niż użycie tradycyjnych linii dzierżawionych.

Technologia sieci VPN pozwala kontrolować i zabezpieczać połączenia z oddziałami firmy, z pracownikami przebywającymi w terenie, z dostawcami lub partnerami handlowymi.

Zastosowania, w których sieć VPN sprawdza się najlepiej, to:
- zdalny dostęp dla użytkowników spoza firmy lub przebywających w terenie,
- połączenia głównej siedziby firmy z komputerami pracowników pracujących w domu i z oddziałami lokalnymi,
- komunikacja między firmami.

W przypadku braku ograniczeń w dostępie użytkowników do newralgicznych systemów mogą pojawić się pewne zagrożenia. Bez opracowania precyzyjnych reguł dostępu do systemu istnieje zagrożenie utraty kontroli nad poufnością danych firmy. Należy opracować plan, który pozwoli ograniczyć dostęp do systemu tylko do tych osób, które muszą wspólnie użytkować dane w systemie. Sieć VPN umożliwia zachowanie kontroli nad przesyłanymi danymi, zapewniając przy tym tak istotne z punktu widzenia ochrony funkcje, jak uwierzytelnianie stron i ochrona poufności danych. Po utworzeniu wielu połączeń VPN w każdym z nich można zdefiniować, kto ma mieć dostęp do których systemów. Na przykład działy księgowości i kadr mogą być połączone poprzez odrębną sieć VPN.

Zezwolenie użytkownikom na łączenie się z systemem poprzez Internet oznacza stworzenie możliwości przepływu ważnych dla firmy informacji przez publicznie dostępne sieci komunikacyjne, gdzie dane te są narażone na ataki. Do metod zabezpieczenia przekazywanych danych należą szyfrowanie oraz uwierzytelnianie komunikujących się stron, co służy ochronie poufności danych i uniemożliwia ingerencję osób niepowołanych. Sieci VPN stanowią rozwiązanie jednego z aspektów ogólnego problemu ochrony danych: zabezpieczenia przepływu danych między systemami. Sieć VPN chroni dane przesyłane między dwoma punktami końcowymi połączenia. Dodatkowo można użyć funkcji reguł pakietów w celu określenia, jakie pakiety IP mogą być przesyłane w ramach sieci VPN.

Sieć VPN można utworzyć w celu zestawienia połączenia, w którym ochronie podlegają dane przekazywane między dwoma zaufanymi punktami, nad którymi mamy kontrolę. Należy jednak nadal zwracać uwagę na zakres dostępu zapewnianego partnerom w sieci VPN. W połączeniu VPN zachodzi szyfrowanie danych przesyłanych przez sieci publiczne. Jednak zależnie od konfiguracji sieci VPN, szyfrowanie może nie dotyczyć danych przesyłanych w obrębie sieci wewnętrznych komunikujących się przez VPN. Z tego powodu należy dokładnie planować konfigurowanie każdego połączenia VPN. Należy upewnić się, że partner sieci VPN otrzymał dostęp tylko do tych hostów lub zasobów sieci wewnętrznej, do których miał go otrzymać.

Na przykład dostawca może potrzebować informacji o częściach znajdujących się na składzie. Informacje te są w bazie danych używanej do aktualizacji stron WWW w sieci intranet. Należy pozwolić dostawcy na bezpośredni dostęp do tych stron poprzez połączenie VPN. Dostawca nie powinien jednak uzyskać dostępu do zasobów systemowych, takich jak sama baza danych. Na szczęście możliwe jest takie skonfigurowanie sieci VPN, aby przepływ danych między dwoma punktami końcowymi odbywał się tylko z użyciem portu 80. Port 80 jest domyślnym portem używanym przez protokół HTTP. Dlatego też dostawca może wysyłać żądania i odbierać odpowiedzi tylko przez to połączenie.

VPN należy do środków ochrony na poziomie sieci, ponieważ możliwe jest zdefiniowanie rodzaju pakietów, jakie mogą być przekazywane w ramach sieci VPN. Sieci VPN nie działają jednak tak jak firewall podczas regulacji przepływu pakietów przychodzących do systemu i wychodzących z niego. Ponadto, technika VPN nie jest jedynym sposobem zabezpieczania komunikacji między systemem iSeries a innymi sieciami. Zależnie od potrzeb, lepszym rozwiązaniem może się okazać protokół SSL.

To, czy ochrona zapewniana przez sieć VPN odpowiada potrzebom, zależy od chronionego obiektu. Zależy także od zmian, które zamierza się wprowadzić w celu zapewnienia tej ochrony. Podobnie jak w przypadku każdej decyzji podejmowanej odnośnie ochrony, należy przemyśleć wpływ sieci VPN na strategię ochrony.

Rozdział 9. Ochrona internetowa - terminologia

Aby ustalić podstawę do dyskusji na temat ochrony internetowej, należy zdefiniować kilka terminów internetowych. Doświadczeni użytkownicy Internetu mogą pominąć ten rozdział.

Authentication (Uwierzytelnianie)
Uwierzytelnianie jest to sprawdzenie, czy zdalny klient lub serwer jest rzeczywiście tym, za kogo się podaje. Stwarza podstawy zaufania do zdalnego węzła sieci, z którym się łączymy.

Cracker (Włamywacz)
Złośliwy haker.

Cryptography (Kryptografia)
Nauka o ochronie danych. Kryptografia pozwala przechowywać informacje lub komunikować się z innymi stronami, przy czym niezainteresowane strony nie powinny rozumieć przechowywanych informacji lub komunikacji. Szyfrowanie transformuje zrozumiały tekst w niezrozumiały ciąg danych (tekst zaszyfrowany). Deszyfrowanie odtwarza zrozumiały tekst z niezrozumiałych danych. Oba procesy wykorzystują formuły matematyczne lub algorytm i tajną sekwencję danych (klucz).

Istnieją dwa rodzaje kryptografii:
- W kryptografii o wspólnym/tajnym kluczu **(symetrycznej)** jeden klucz jest wspólny dla obu stron komunikacji. Do szyfrowania i deszyfrowania służy ten sam klucz.
- W kryptografii klucza publicznego **(asymetrycznej)** podczas szyfrowania i deszyfrowania używa się różnych kluczy. Każda strona posiada dwa klucze: publiczny i prywatny. Oba klucze są matematycznie powiązane, jednak uzyskanie klucza prywatnego z klucza publicznego jest praktycznie niemożliwe. Komunikat zaszyfrowany za pomocą czyjegoś klucza publicznego może zostać odszyfrowany tylko za pomocą odpowiedniego klucza prywatnego. Alternatywnie serwer albo użytkownik mogą użyć klucza prywatnego do ″podpisywania″ dokumentów i klucza publicznego do deszyfrowania podpisu cyfrowego. Dzięki temu mechanizmowi można sprawdzać pochodzenie dokumentu.

Digital certificate (Certyfikat cyfrowy)
Certyfikat cyfrowy jest to dokument elektroniczny, który potwierdza tożsamość właściciela certyfikatu w podobny sposób jak paszport. Zaufana strona pośrednicząca, nazywana ośrodkiem certyfikacji, wydaje certyfikaty cyfrowe dla użytkowników i serwerów. Zaufanie do ośrodka certyfikacji stanowi fundament zaufania do certyfikatu jako dokumentu uwierzytelniającego. Dokument można stosować do:
- identyfikacji - kim jest użytkownik,
- uwierzytelniania - upewniania się, że użytkownik jest tym, za kogo się podaje,
- integralności - określania, czy zawartość dokumentu została zmieniona lub do sprawdzania cyfrowego ″podpisu″ nadawcy,
- nieodrzucania - zagwarantowania, że użytkownik nie może udawać, że nie wykonał jakiegoś działania. Na przykład użytkownik nie może kwestionować autoryzacji zamówienia za pomocą karty kredytowej.

Digital signature (Podpis cyfrowy)
Podpis cyfrowy na dokumencie elektronicznym jest odpowiednikiem podpisu osobistego na zwykłym dokumencie. Podpis cyfrowy stanowi dowód pochodzenia dokumentu. Właściciel certyfikatu ″podpisuje″ dokument używając klucza prywatnego związanego z certyfikatem. Odbiorca dokumentu korzysta z odpowiedniego klucza publicznego do deszyfrowania podpisu, który weryfikuje nadawcę jako źródło.

Menedżer certyfikatów cyfrowych (Digital Certificate Manager - DCM)
Digital Certificate Manager pozwala systemowi OS/400 pełnić rolę lokalnego ośrodka certyfikacji (Certificate Authority - CA). Za pomocą DCM można utworzyć certyfikaty cyfrowe dla serwerów lub użytkowników. Możliwe jest importowanie certyfikatów cyfrowych wystawianych przez inne CA.

Certyfikat cyfrowy można powiązać z profilem użytkownika systemu OS/400. Programu DCM można użyć do skonfigurowania aplikacji, tak aby używały one protokołu SSL do chronionej komunikacji.

Distinguished name (Nazwa wyróżniająca)
Nazwa wyróżniająca jest nazwą osoby lub serwera, dla którego ośrodek certyfikacji ma wydać certyfikat cyfrowy. Dzięki temu, że certyfikat zawiera tę nazwę, można wskazać właściciela certyfikatu. W zależności od strategii ośrodka certyfikacji wydającego certyfikat, nazwa wyróżniająca może zawierać inne informacje o uprawnieniach.

Domain name server (Serwer nazw domen - DNS)
Host internetowy konwertujący nazwy internetowe na adresy IP, często we współpracy z innymi serwerami nazw domen w sieci Internet. Na przykład, wiele serwerów DNS może rozpoznawać adres

```
vnet.ibm.com
```

lecz tylko niektóre znają adres IP dla:

```
system1.vnet.ibm.com
```

Przy podłączaniu się do Internetu klient sieci korzysta z serwera nazw domen w celu określenia adresu IP dla systemu hosta, z którym chce się komunikować.

Encryption (Szyfrowanie)
Szyfrowanie przekształca dane do formatu, który nie może być odczytany przez nikogo, kto nie posiada odpowiedniej metody deszyfrowania. Nieuprawnione strony nadal są w stanie przechwycić informacje. Jednakże bez odpowiedniej metody deszyfrowania informacje te są bezużyteczne.

Extranet (Sieć Extranet)
Prywatna sieć firmowa kilku współpracujących organizacji znajdujących się na zewnątrz firewalla firmy. Usługa extranet używa istniejącej infrastruktury sieci Internet, w tym standardowych serwerów, klientów poczty elektronicznej i przeglądarek WWW. Dzięki temu sieć extranet jest bardziej ekonomiczna niż tworzenie i obsługa własnej sieci. Umożliwia korzystanie z rozszerzonych możliwości Internetu współpracującym partnerom handlowym, dostawcom i klientom, co pozwala utrzymywać zarówno bliskie stosunki handlowe, jak i silne więzy komunikacyjne.

Firewall
Logiczna bariera pomiędzy siecią wewnętrzną a siecią zewnętrzną, taką jak Internet. Firewall składa się z jednego lub wielu systemów oprogramowania i sprzętu. Steruje dostępem oraz przepływem informacji pomiędzy systemami chronionymi i zaufanymi oraz systemami niechronionymi i niezaufanymi.

Hacker (Haker)
Każda nieupoważniona osoba, która próbuje włamać się do systemu.

Hypertext Links (Odsyłacze hipertekstowe)
Sposób prezentacji informacji elektronicznej z połączeniami (zwanymi odsyłaczami hipertekstowymi) pomiędzy jedną informacją (zwaną węzłem hipertekstowym) a inną.

Hypertext markup language (HTML)
Język używany do definiowania dokumentów hipertekstowych. Języka HTML można używać do określania wyglądu dokumentu (takich elementów, jak wyróżnienia i styl czcionki) i sposobu połączenia go z innymi dokumentami lub obiektami.

Hypertext transport protocol (HTTP)
Standardowa metoda dostępu do dokumentów hipertekstowych.

Internet
Ogólnoświatowa “sieć sieci” połączonych między sobą. A także zestaw współpracujących aplikacji, które pozwalają komputerom podłączonym do ″sieci sieci″ komunikować się. Internet udostępnia cały szereg usług, takich jak przeglądanie informacji, przesyłanie plików, poczta elektroniczna, zdalne logowanie, grupy dyskusyjne i inne usługi. Internet jest często określany jako “sieć”.

Internet client (Klient internetowy)
Program (lub użytkownik) wykorzystujący sieć Internet do tworzenia żądań i odbierania wyników od programu serwera internetowego. Różne programy klientów mogą żądać różnych typów usług internetowych. Przeglądarka WWW jest przykładem programu klienckiego, podobnie jak FTP (File transfer protocol).

Internet host (Host internetowy)
Komputer podłączony do sieci intranet lub Internet. Na hoście internetowym może działać kilka programów serwerów internetowych. Na przykład na hoście internetowym może działać serwer FTP odpowiadający na żądania aplikacji klientów FTP. Na tym samym hoście może działać serwer HTTP odpowiadający na żądania klientów korzystających z przeglądarek WWW. Programy serwera zwykle działają w tle (jako zadania wsadowe) systemu hosta.

Internet key exchange (IKE)
Protokół IKE używany wraz z IPSec obsługuje automatyczne uzgadnianie Security Associations, a także automatyczne generowanie i odświeżanie kluczy szyfrujących. Ogólnie, protokoły IKE są używane jako część sieci VPN.

Internet name (Nazwa internetowa)
Alias adresu IP. Adres IP ma złożoną formę numeryczną i trudno go zapamiętać, na przykład 10.5.100.75. Można przypisać ten adres IP do nazwy internetowej, na przykład

```
system1.vnet.ibm.com
```

Nazwa internetowa jest też określana jako w pełni kwalifikowana nazwa domeny. W reklamie: “Odwiedź naszą stronę główną” adres strony głównej zawiera nazwę internetową, nie zaś adres IP, ponieważ nazwę internetową łatwiej zapamiętać.

W pełni kwalifikowana nazwa domeny składa się z kilku części. Na przykład:

```
system1.vnet.ibm.com
```

składa się z następujących części

com: Wszystkie sieci komercyjne. przez organizację *Internet* (organizację zewnętrzną). Różne oznaczenia są przypisywane do różnych rodzajów sieci (na przykład com oznacza instytucje komercyjne, a edu edukacyjne).

ibm: Identyfikator organizacji. Ta część nazwy domeny jest także nadawana przez organizację Internet i jest unikalna. Tylko jedna organizacja na świecie może mieć identyfikator

```
ibm.com
```

vnet: Grupa systemów wewnątrz

```
ibm.com
```

Ten identyfikator jest przydzielany wewnętrznie. Administrator ibm.com może utworzyć jedną lub wiele grup.

system1:
Nazwa hosta internetowego wewnątrz grupy vnet.ibm.com.

Internet server (Serwer internetowy)
Program (lub zestaw programów) akceptujący żądania od odpowiednich programów klientów w sieci Internet i odpowiadający tym klientom poprzez sieć Internet. Serwer internetowy można rozumieć jako punkt, który klient internetowy może odwiedzać (uzyskiwać do niego dostęp). Serwery udostępniają różne usługi, do których zaliczają się:

- Przeglądanie (“strona główna” i odsyłacze do innych dokumentów i obiektów).
- Przesyłanie plików. Klient może zażądać, na przykład, przesłania plików z serwera do klienta. Mogą to być aktualizacje oprogramowania, listy produktów lub dokumenty.
- Handel elektroniczny, np. możliwość żądania informacji lub zamawiania produktów.

Internet service provider (ISP) (Dostawca usług internetowych)
Organizacja zapewniająca połączenie z siecią Internet w mniej więcej taki sposób, w jaki lokalna firma telefoniczna zapewnia połączenie z ogólnoświatowymi sieciami telefonicznymi.

Intranet
Wewnętrzna sieć w organizacji, w której korzysta się z narzędzi internetowych, takich jak przeglądarki WWW czy protokół FTP.

IP address (Adres IP)
Adres IP (Internet Protocol) to sposób identyfikacji w sieci TCP/IP (Internet jest bardzo dużą siecią TCP/IP). Serwer internetowy zwykle ma przypisany unikalny adres IP. Klient internetowy może korzystać z tymczasowego, lecz unikalnego adresu IP przydzielonego przez dostawcę usług internetowych.

IP datagram (Datagram IP)
Jednostka informacji wysyłana w sieci TCP/IP. Datagram IP (nazywany też pakietem) zawiera dane oraz informacje nagłówka, takie jak adres IP punktów źródłowego i docelowego.

IP filters (Filtry IP)
Filtrowanie IP stanowi podstawowy mechanizm ochronny firewalla. Pozwala określić, jakie pakiety są przepuszczane przez firewall (na podstawie szczegółów sesji IP). Dzięki temu sieć chroniona jest przed napastnikami z zewnątrz używającymi nieskomplikowanych technik (takich jak poszukiwanie serwerów chronionych) i bardziej skomplikowanych technik (takich jak oszukiwanie poprzez adres IP). Filtrowanie należy traktować jako podstawę, na której konstruowane są inne narzędzia. Zapewnia infrastrukturę, w której działają te narzędzia, i zabrania dostępu wszystkim oprócz najbardziej zdeterminowanych włamywaczy.

IPSec Zestaw protokołów obsługujących chronioną wymianę pakietów w warstwie IP. IPSec jest zestawem standardów, których używa iSeries i wiele innych systemów do tworzenia sieci VPN.

IP spoofing (Oszukiwanie poprzez adres IP)
Próba uzyskania dostępu do systemu przez udawanie zaufanego systemu (adresu IP). Intruz konfiguruje system, któremu nadaje adres IP zaufanego systemu. Wytwórcy routerów opracowali zabezpieczenia, które wykrywają i odrzucają próby oszukiwania.

Network address translation (NAT) (Translacja adresu sieciowego)
Stanowi bardziej przezroczystą alternatywę serwerów proxy i SOCKS. Upraszcza także konfigurowanie sieci, umożliwiając łączenie sieci o niekompatybilnych strukturach adresowania. NAT zapewnia dwie główne funkcje. Może chronić publiczny serwer WWW, który ma działać w sieci wewnętrznej, i zapewnia ochronę poprzez umożliwienie ukrycia prawdziwego adresu serwera za adresem, który jest dostępny publicznie. Zapewnia także mechanizm dostępu do Internetu użytkownikom wewnętrznym, ukrywając prywatny wewnętrzny adres IP. NAT zapewnia ochronę, gdy wewnętrzni użytkownicy uzyskują dostęp do usług Internetu, ponieważ ich prywatne adresy są ukryte.

Non-repudiation (Nieodrzucanie)
Nieodrzucanie (non-repudiation) jest dowodem na to, że transakcja miała miejsce albo że komunikat został wysłany lub odebrany. Korzystanie z certyfikatów cyfrowych lub szyfrowania według klucza publicznego w celu ″podpisywania″ transakcji, komunikatów i dokumentów zapewnia nieodrzucanie.

Packet (Pakiet)
Datagram zawierający informacje o protokole linii, takim jak Ethernet, Token Ring lub frame-relay.

Proxy (Serwer proxy)
Serwer proxy to aplikacja TCP/IP przesyłająca żądania i odpowiedzi pomiędzy klientami w chronionej sieci wewnętrznej i serwerami w sieci niezaufanej. Serwer proxy przerywa połączenie TCP/IP, aby ukryć informacje o sieci wewnętrznej (takie jak adresy IP). Hosty poza siecią wewnętrzną postrzegają serwer proxy jako źródło komunikacji.

Public key infrastructure (PKI) (Infrastruktura klucza publicznego)
System certyfikatów cyfrowych, ośrodków certyfikacji i innych ośrodków rejestracyjnych, weryfikujący i sprawdzający poprawność każdej strony uczestniczącej w transakcji internetowej.

Secure Sockets Layer (SSL)
Protokół SSL, opracowany przez firmę Netscape, jest obecnie standardem szyfrowania sesji pomiędzy klientem a serwerem. SSL korzysta z symetrycznego szyfrowania kluczy do szyfrowania sesji pomiędzy serwerem i klientem (użytkownikiem). Klient i serwer negocjują klucz sesji podczas wymiany certyfikatów cyfrowych. Dla każdego klienta i dla każdej sesji serwera SSL jest tworzony inny klucz. Nawet gdyby nieupoważnieni użytkownicy przechwycili i odszyfrowali klucz sesji (co jest mało prawdopodobne), to nie będą go mogli używać do podsłuchiwania równoczesnych, późniejszych czy wcześniejszych sesji.

Sniffing (Węszenie)
Monitorowanie i podsłuchiwanie transmisji elektronicznych. Informacje wysyłane przez sieć Internet mogą przechodzić przez wiele routerów, zanim osiągną punkt docelowy. Wytwórcy, dostawcy usług internetowych i twórcy systemów operacyjnych włożyli wiele wysiłku, aby zapewnić, że w rdzeniu sieci Internet węszenie będzie niemożliwe. Udane przypadki węszenia są coraz rzadsze. Większość z nich zdarza się w prywatnych sieciach LAN, które są podłączone do sieci Internet, nie zaś do samego rdzenia sieci. Jednak należy być świadomym możliwości węszenia, ponieważ większość transmisji TCP/IP jest niezaszyfrowana.

SOCKS
Architektura klient/serwer, która transportuje przepływ pakietów TCP/IP przez chronioną bramę. Serwer SOCKS wykonuje wiele takich samych usług jak serwer proxy.

Spoofing (Oszukiwanie)
Atakujący podszywają się pod system zaufany i próbują skłonić system do wysłania im tajnych informacji.

TCP/IP
Główny protokół komunikacyjny używany w sieci Internet. TCP/IP to skrót od Transmission Control Protocol/Internet Protocol. Protokołu TCP/IP można także używać w sieci wewnętrznej.

Trojan horse (Koń trojański)
Koń trojański to program komputerowy, który pozornie jest użyteczny i nieszkodliwy. Zawiera jednak ukryte funkcje, które korzystają z uprawnień przypisanych użytkownikowi podczas uruchomienia programu. Może to być na przykład skopiowanie wewnętrznych informacji o uprawnieniach z komputera, na którym został uruchomiony, i przesłanie ich do twórcy konia trojańskiego.

Virtual private network (Sieć VPN)
Rozszerzenie prywatnych sieci intranetowych przedsiębiorstwa. Z sieci VPN można korzystać w sieciach publicznych, na przykład w sieci Internet, tworząc chronione połączenia prywatne poprzez utworzenie ″tunelu″ prywatnego. Sieci VPN bezpiecznie przesyłają informacje przez sieć Internet, łącząc z danym systemem innych użytkowników. Zaliczają się do nich:
- zdalni użytkownicy,
- biura oddziałów,
- partnerzy handlowi i dostawcy.

Web browser (Przeglądarka WWW)
Aplikacja klienta HTTP. Przeglądarka WWW interpretuje język HTML, aby wyświetlać użytkownikowi dokumenty hipertekstowe. Użytkownik może uzyskać dostęp do obiektu, do którego odnosi się odsyłacz, klikając (wybierając) obszar w bieżącym dokumencie. Obszar ten jest często nazywany **gorącym punktem**. Przykładami przeglądarek WWW są Internet Connection Web Explorer i Netscape Navigator.

World Wide Web (Sieć WWW)
Sieć połączonych ze sobą serwerów i klientów używających standardowego formatu tworzenia dokumentów (HTML) i sposobu dostępu do dokumentów (HTTP). Ta sieć połączeń, zarówno z serwera do serwera, jak i z dokumentu do dokumentu, jest nazywana **Siecią**.