Systémy IBM - iSeries

# Zabezpečení iSeries a zabezpečení Internetu

*Verze 5, vydání 4*

Systémy IBM - iSeries

# Zabezpečení iSeries a zabezpečení Internetu

*Verze 5, vydání 4*

**Poznámka**

Dříve než použijete tyto informace a produkt, který podporují, nezapomeňte si přečíst informace uvedené v části “Upozornění”, na stránce 35.

**Sedmé vydání (únor 2006)**

Toto vydání se týká verze 5, vydání 4, modifikace 0 operačního systému IBM i5/OS (5722-SS1) a všech následných vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nefunguje na všech modelech počítačů RISC (reduced instruction set computer) ani na modelech CISC.

# Obsah

# iSeries a zabezpečení Internetu

Přístup k Internetu ze sítě LAN je významným krokem v rozvoji vaší sítě, který bude vyžadovat, abyste přehodnotili své požadavky na zabezpečení ochrany dat.

Naštěstí má server IBM @server iSeries integrované softwarové řešení a architekturu zabezpečení, pomocí nichž si můžete vybudovat silnou ochranu proti možným nástrahám a vetřelcům, ohrožujících bezpečnost vašich dat v síti Internet. Správné používání těchto nabízených bezpečnostních opatření serveru iSeries zajistí, aby vaši zákazníci, zaměstnanci a obchodní partneři od vás získali potřebné informace a mohli s vámi spolupracovat v zabezpečeném prostředí.

Informace, které zde najdete, vás poučí o známých okolnostech představujících ohrožení v oblasti zabezpečení ochrany dat a o tom, jaký mají tato rizika vztah k vašim cílům v internetovém a elektronickém podnikání. Dozvíte se také, jak odhadnout riziko ve srovnání s přínosem použití různých voleb zabezpečení ochrany dat, která pro práci s těmito riziky nabízí server iSeries. A konečně můžete určit, jak tyto informace využít při vývoji plánu pro zabezpečení ochrany dat, který by odpovídal potřebám vašeho podnikání

## Tisk PDF

V této části najdete informace, jak zobrazit a vytisknout PDF verzi této publikace.

Chcete-li zobrazit nebo stáhnout tento dokument ve formátu PDF, vyberte téma iSeries a zabezpečení Internetu (416 KB nebo 60 stran).

Zobrazovat nebo stahovat můžete také tato související témata:

- Intrusion Detection (cca 160 KB). Můžete nastavit zásady detekce vniknutí, které budou monitorovat události podezřelých vniknutí, která byla provedena prostřednictvím TCP/IP sítě, jako např. nesprávně vytvořené IP pakety. Můžete také napsat aplikaci, která bude analyzovat data monitorování a hlásit administrátorovi zabezpečení každé případné probíhající TCP/IP vniknutí.
- EIM (Enterprise Identity Mapping) (cca 700 KB). EIM (Enterprise Identity Mapping) je mechanismus mapování osoby nebo entity (jako např. služby) na odpovídající totožnosti uživatelů v různých registrech uživatelů v celém podniku.
- SSO (Single signon) (cca 600 KB). Řešení pro jednotné přihlášení snižuje počet přihlášení, které musí uživatel provést, stejně jako počet hesel, které uživatel potřebuje k přístupu k více aplikacím a serverům.
- Plánování a nastavení zabezpečení systému (cca 3500 KB).

### Uložení souborů ve formátu PDF

Jak uložit soubory ve formátu PDF na pracovní stanici za účelem prohlížení nebo tisku:

1. Klepněte pravým tlačítkem myši na PDF dokument ve vašem prohlížeči (klepněte pravým tlačítkem myši na výše uvedený odkaz).
2. Klepněte na volbu, která soubor PDF uloží lokálně.
3. Přejděte do adresáře, do kterého chcete uložit soubor PDF.
4. Klepněte na **Save** (Uložit).

### Stažení aplikace Adobe Reader

Chcete-li si prohlížet nebo tisknout uvedené dokumenty ve formátu PDF, musíte mít na svém systému nainstalován produkt Adobe Reader. Bezplatnou kopii tohoto programu si můžete stáhnout z webových stránek společnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

**Související pojmy**

Detekování vniknutí

Enterprise Identity Mapping (EIM)

Jednotné přihlášení

Plánování a nastavení zabezpečení systému

---

## Faktory zabezpečení systému iSeries a Internetu

Zde naleznete přehled silných stránek zabezpečení ochrany dat systému iSeries a nabídky zabezpečení ochrany dat.

Odpověď na otázku ″Co bych měl vědět o zabezpečení ochrany dat a o Internetu?″ je, že to závisí na tom, jak chcete používat Internet. Problémy týkající se zabezpečení Internetu jsou významné. Problémy, kterými se budete zabývat, závisí na tom, jak hodláte používat Internet. Vaší první akcí v síti Internet by mohlo být umožnit uživatelům interní sítě přístup k WWW a k elektronické poště přes Internet. Možná budete potřebovat také schopnost přenášet citlivé informace z jednoho uzlu do druhého. A konečně můžete plánovat použití Internetu pro elektronický obchod nebo pro vytvoření sítě typu extranet mezi vaší firmou a obchodními partnery a dodavateli.

Dříve než s Internetem začnete, měli byste si promyslet, co chcete dělat a jakým způsobem to chcete dělat. Rozhodování ve věci využití Internetu a zabezpečení dat na Internetu může být složité. Při vytváření plánu využití Internetu vám může pomoci téma *Scénář: Plán elektronického podnikání firmy JKL Toy* v rámci aplikace IBM Systems Software Information Center. (Poznámka: Jestliže nejste obeznámeni s terminologií týkající se zabezpečení dat a Internetu, můžete se při práci s tímto materiálem podívat na běžnou *terminologii zabezpečení dat* v aplikaci IBM Systems Software Information Center.)

Jakmile si ujasníte, jak chcete používat Internet pro elektronické podnikání a také jaké jsou problémy zabezpečení ochrany dat a dostupné nástroje, funkce a nabídky produktů, můžete vyvinout vlastní strategii a cíle zabezpečení ochrany dat. Vaše volby při vyvíjení strategie zabezpečení ochrany dat bude ovlivňovat řada faktorů. Když se svou organizací pronikáte na Internet, představuje strategie zabezpečení ochrany dat rozhodující faktor pro zajištění bezpečnosti vašich systémů a prostředků.

### Charakteristika zabezpečení ochrany dat na serveru iSeries

Kromě velké nabídky specifických produktů sloužících k zabezpečení vašeho systému v síti Internet má server iSeries velmi účinné charakteristiky zabezpečení systému, jako například:

- Integrované zabezpečení dat se nesmírně obtížně obchází, srovnáme-li je s nabídkami přídavných softwarových balíků v jiných systémech.
- Objektová architektura, která technicky ztěžuje vytvoření a rozšíření viru. Na serveru iSeries nemůže soubor předstírat, že je program, a program nemůže změnit jiný program. Vlastnosti integrity systému iSeries vyžadují, abyste při přístupu k objektům použili systémem dodávaná rozhraní. K objektu nemůžete přistupovat přímo podle jeho adresy v systému. Nelze vzít offset a změnit jej na ukazatel nebo z něj ukazatel ″vyrobit″. Manipulace s ukazateli je oblíbená technika hackerů v architektuře jiných systémů.
- Flexibilita, která vám umožňuje nastavit zabezpečení systému tak, aby vyhovovalo vašim specifickým požadavkům. Můžete použít program @server Security Planner , který doporučí zabezpečení ochrany dat odpovídající potřebám vaší organizace.

### Rozšířená nabídka produktů pro zabezpečení ochrany dat systému iSeries

Systém iSeries také nabízí několik specifických produktů pro zabezpečení ochrany dat, které můžete použít k rozšíření zabezpečení systému, když se připojujete k síti Internet. Podle toho, jak Internet používáte, budete se rozhodovat pro využití některých z těchto nabízených produktů:

- VPN (Virtual Private Network) je rozšířením soukromé vnitropodnikové sítě do veřejné sítě, jakou je například Internet. Chcete-li vytvořit zabezpečené soukromé připojení, můžete k tomu použít VPN a v podstatě vytvořit soukromý ″tunel″ do veřejné sítě. VPN je integrovaná funkce systému i5/OS dostupná z prostředí produktu iSeries Navigator. Další informace o sítích VPN najdete v tématu ″VPN (Virtual Private Networking)″ v aplikaci IBM Systems Software Information Center.
- Pravidla paketu je integrovaná funkce systému i5/OS dostupná z prostředí produktu iSeries Navigator. Tato funkce vám umožňuje konfigurovat pravidla pro filtrování IP paketů a pro NAT (převod síťových adres) pro řízení postupu provozu TCP/IP do a ze serveru iSeries. Další informace o pravidlech paketů najdete v tématu ″Pravidla paketu″ v aplikaci IBM Systems Software Information Center.
- Zabezpečení komunikace aplikací pomocí SSL (Secure Sockets Layer) vám umožňuje nakonfigurovat aplikace tak, aby používaly protokol SSL k vytvoření zabezpečeného spojení mezi aplikacemi serverů a jejich klienty. Funkce SSL byla původně vyvinuta pro zabezpečený prohlížeč WWW a aplikace serveru, je však možné povolit i jiným aplikacím, aby ji používaly. Řada aplikací serveru iSeries má nyní povoleno používat protokol SSL, včetně produktů IBM HTTP Server for iSeries, iSeries Access Express, File Transfer Protocol (FTP), Telnet a další. Další informace o protokolu SSL najdete v tématu ″Zabezpečení aplikací pomocí SSL″ v aplikaci IBM Systems Software Information Center.

Jakmile si ujasníte, jak chcete používat Internet, a také jaké jsou problémy zabezpečení dat a jaké nástroje ochrany, funkce a nabídky produktů jsou dostupné, budete připraveni vyvinout vlastní strategii a cíle zabezpečení ochrany dat. Vaše volby při vyvíjení strategie zabezpečení ochrany dat bude ovlivňovat řada faktorů. Když svou organizaci rozšiřujete na Internet, představuje strategie zabezpečení ochrany dat rozhodující faktor pro zajištění bezpečnosti vašeho systému.

**Poznámka:** Chcete-li zjistit podrobnější informace o tom, jak začít používat Internet pro podnikatelské účely, podívejte se na:

- téma *Připojení k Internetu* v aplikaci IBM Systems Software Information Center
- červenou knihu *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929)

**Související pojmy**

“Strategie a cíle zabezpečení ochrany dat” na stránce 6
Definice, co se má chránit, a co lze očekávat od uživatelů.

## Plánování zabezpečení Internetu

Poskytuje informace, s jejichž pomocí vytvoříte zásady zabezpečení pro pokrytí vašich požadavků na zabezpečení Internetu.

Při vývoji plánů na použití sítě Internet musíte pečlivě naplánovat i potřeby jeho zabezpečení. Musíte shromáždit podrobné informace o plánovaném využití Internetu a zdokumentovat konfiguraci vaší interní sítě. Na bázi výsledků těchto shromážděných informací můžete dospět k přesnému ohodnocení požadavků na zabezpečení ochrany dat.

Měli byste například zdokumentovat a popsat následující skutečnosti:

- Aktuální konfiguraci vaší sítě.
- Informace o konfiguraci serveru DNS a serveru elektronické pošty.
- Vaše připojení k poskytovateli služeb sítě Internet (ISP).
- Jaké internetové služby chcete používat.
- Jaké služby chcete poskytovat uživatelům Internetu.

Zdokumentování takových informací vám pomůže určit, kde jsou bezpečnostní rizika a jaká bezpečnostní opatření musíte použít, abyste tato rizika minimalizovali.

Například se rozhodnete, že chcete interním uživatelům dovolit používat Telnet, budou-li se chtít připojit ke speciálnímu zdroji za účelem výzkumu. Vaši interní uživatelé tuto službu potřebují při vývoji nových produktů v podniku. Máte však jisté obavy o důvěrná data, která by nechráněná procházela sítí Internet. Kdyby se konkurence k těmto datům dostala a zneužila jich, mohlo by to pro vaši společnost představovat finanční riziko. Když určíte potřeby vašeho využití (Telnet) a s ním spojené riziko (ohrožení důvěrných informací), můžete rozhodnout, jaká další bezpečnostní opatření byste měli implementovat pro zajištění utajení dat při tomto využití (aktivace SSL (Secure Sockets Layer)).

Při práci na vývoji plánu využití sítě Internet a plánu pro zabezpečení ochrany dat vám mohou pomoci tato témata:

- Téma *Metoda zabezpečení ochrany dat pomocí vrstvené obrany* podává informace o otázkách spojených s vytvořením vyčerpávajícího plánu pro zabezpečení ochrany dat.
- Téma *Strategie a cíle zabezpečení ochrany dat* podává informace, které vám pomohou určit, co byste měli z dokumentovat jako součást vaší strategie zabezpečení ochrany dat.
- Téma *Scénář: Plán elektronického podnikání firmy JKL Toy* poskytuje praktický model typického využití Internetu a plánu pro zabezpečení ochrany dat, který můžete využít při tvorbě vlastního plánu.

## Metoda zabezpečení ochrany dat pomocí vrstvené obrany

**Strategie zabezpečení ochrany dat** definuje to, co chcete ochránit a to, co očekáváte od uživatelů vašeho systému.

Je základem plánu pro zabezpečení ochrany dat při navrhování nových aplikací nebo rozšiřování vaší stávající sítě. Popisuje odpovědnost uživatelů, jako například ochranu důvěrných informací a vytváření složitých hesel.

**Poznámka:** Ve své organizaci musíte vytvořit a prosadit strategii zabezpečení ochrany dat, která minimalizuje riziko pro vaši interní síť. Inherentní funkce zabezpečení dat serveru iSeries, jsou-li správně nakonfigurovány, vám poskytnou možnost minimalizovat mnohá rizika. Když připojíte systém iSeries k síti Internet, budete muset učinit další bezpečnostní opatření, aby byla zajištěna bezpečnost vaší interní sítě.

Mnohá rizika jsou spojena s používáním přístupu k Internetu k provádění obchodní činnosti. Kdykoli budete vytvářet strategii zabezpečení ochrany dat, musíte vytvořit rovnováhu mezi poskytováním služeb a řízením přístupu k funkcím a datům. U počítačů zapojených do sítí je zabezpečení mnohem obtížnější, protože útoku je vystaven samotný komunikační kanál.

Některé internetové služby jsou zranitelnější vůči jistým typům napadení než jiné. Je proto rozhodující, abyste pochopili rizika spojená s jednotlivými službami, které máte v úmyslu použít nebo poskytovat. Mimoto, když pochopíte možná bezpečnostní rizika, budete moci jasně určit cíle zabezpečení dat.

Internet hostí mnoho jedinců, kteří představují ohrožení pro komunikaci v této síti. Následující seznam popisuje některá typická bezpečnostní rizika, se kterými se můžete setkat:

- **Pasivní napadení**: Při pasivním napadení vetřelec prostě sleduje provoz ve vaší síti a pokouší se odhalit utajované skutečnosti. Taková napadení mohou být buď v síti (vystopování komunikační linky), nebo v systému (nahrazení systémové komponenty programem typu trojský kůň, který záludně krade data). Pasivní napadení se odhaluje nejobtížněji. Měli byste proto předpokládat, že někdo špehuje všechno, co po Internetu posíláte.
- **Aktivní napadení:** Při aktivním napadení se vetřelec pokouší porušit vaši obranu a proniknout do systémů vašich sítí. Existuje několik typů aktivního napadení:
  - Při **pokusech o přístup do systému** se vetřelec pokouší využít nedostatky v zabezpečení, aby získal přístup k systému klienta nebo serveru ovládl je.
  - Při napadení typu **spoofing** se vetřelec pokouší překonat vaši obranu předstíráním, že jde o důvěryhodný systém, nebo vás nějaký uživatel přesvědčí, abyste mu poslali utajované informace.
  - Při **útocích s následkem přerušení síťových služeb** se vetřelec pokouší zasahovat do vašich operací nebo je ukončit tak, že přesměruje provoz nebo zavalí systém spoustou nevyžádaných dat.

– Při **šifrovacích napadeních** se vetřelec pokusí uhodnout nebo ukrást vaše hesla nebo použije specializované nástroje, aby dešifroval zašifrovaná data.

## Mnohovrstvá obrana

Protože se potenciální rizika zabezpečení Internetu mohou vyskytnout na nejrůznějších úrovních, musíte podniknout taková bezpečnostní opatření, která zabezpečí proti riziku více obranných vrstev. Obecně by vás po připojení k Internetu nemělo překvapit, **jestliže** zaznamenáte pokusy o vniknutí do systému nebo útoky s následkem přerušení síťových služeb. Místo toho byste měli předpokládat, že **určitě** dojde k problému se zabezpečením dat. V důsledku toho se jako nejlepší obrana jeví promyšlený, předvídavý útok. Použití vrstveného přístupu při plánování strategie zabezpečení Internetu zajistí, že jestliže vetřelec pronikne jednou obrannou vrstvou, bude zastaven vrstvou následující.

Vaše strategie zabezpečení ochrany dat by měla zahrnovat opatření, která poskytují ochranu přes tyto vrstvy modelu tradičního síťového počítačového zpracování. Obecně řečeno byste měli plánovat zabezpečení dat od těch nejzákladnějších (zabezpečení na úrovni systému) až po ta nejsložitější (zabezpečení na úrovni transakce).

**Zabezpečení na úrovni systému**
Opatření pro zabezpečení systému představují poslední obrannou linii proti problémům s bezpečností v síti Internet. V důsledku toho musí být vaším prvním krokem v celkové strategii zabezpečení Internetu řádná konfigurace výkonných zabezpečení základního systému. Téma Úrovně zabezpečení systému v rámci základní přípravy na připojení k Internetu popisuje, jaká nastavení by měl uživatel pro připojení k Internetu použít.

**Zabezpečení na úrovni sítě**
Opatření pro zabezpečení sítě řídí přístup k vašemu systému iSeries a k jiným systémům v síti. Když připojíte síť k Internetu, měli byste učinit odpovídající opatření pro zabezpečení na úrovni sítě vhodná k ochraně vašich interních prostředků v síti před neoprávněným přístupem a vniknutím. Nejběžnějším prostředkem pro zajištění bezpečnosti sítě je ochranná bariéra. Poskytovatel služeb sítě Internet (ISP) by měl představovat důležitý prvek v plánu zabezpečení vaší sítě. Schéma zabezpečení sítě by mělo vymezit, jaká bezpečnostní opatření zajistí poskytovatel služeb sítě Internet (ISP), například pravidla pro připojení směrovače ISP a opatření pro služby jmen domény (DNS). Téma Volby zabezpečení sítě popisuje bezpečnostní opatření, o jejichž implementaci na úrovni sítě byste měli uvažovat, chcete-li zajistit ochranu vašich interních prostředků.

**Zabezpečení na úrovni aplikace**
Opatření pro zabezpečení na úrovni aplikace řídí, jak mohou uživatelé zacházet se specifickými aplikacemi. Obecně byste měli konfigurovat nastavení zabezpečení u každé aplikace, kterou používáte. Zvláštní péči byste však měli věnovat nastavení zabezpečení dat u těch aplikací a služeb, které budete na Internetu využívat nebo do něj poskytovat. Takové aplikace a služby jsou citlivé na zneužití ze strany neoprávněných uživatelů hledajících způsob, jak získat přístup do systémů vaší sítě. Opatření pro zabezpečení dat, která se rozhodnete použít, musí pokrýt ohrožení na straně serveru i na straně klienta. Téma Volby zabezpečení na úrovni aplikace popisuje rizika zabezpečení a dostupné volby, které jim mohou zamezit, u řady populárních internetových aplikací a služeb.

**Zabezpečení na úrovni přenosu**
Opatření pro zabezpečení na úrovni přenosu chrání datové komunikace uvnitř sítě a mezi sítěmi. Při komunikaci v nedůvěryhodné síti, jakou je Internet, nemůžete ovládat postup provozu ze zdroje na místo určení. Váš provoz a přenášená data postupují přes mnoho různých serverů, které nemůžete ovládat. Pokud nenastavíte opatření pro zabezpečení dat, jako například konfigurování vlastních aplikací tak, aby používaly SSL (Secure Sockets Layer), bude si vaše směrovaná data moci kdokoliv prohlédnout a použít. Opatření pro zabezpečení dat na úrovni přenosu chrání vaše data, když procházejí mezi hranicemi další úrovně zabezpečení. Téma Volby zabezpečení na úrovni přenosu podává informace o bezpečnostních opatřeních, která můžete implementovat a jejichž prostřednictvím můžete ochránit data, když procházejí přes nedůvěryhodné sítě, jako je například Internet.

Při vývoji celkové strategie zabezpečení ochrany dat v síti Internet byste měli vyvinout strategii pro každou vrstvu jednotlivě. A kromě toho byste měli popsat, jaká bude interakce jedné strategické sady s ostatními, aby poskytovala úplnou bezpečnostní síť pro vaše podnikání.

**Související pojmy**

**Související odkazy**

Terminologie zabezpečení

# Strategie a cíle zabezpečení ochrany dat

Definice, co se má chránit, a co lze očekávat od uživatelů.

## Vaše strategie zabezpečení ochrany dat

Každá internetová služba, kterou používáte nebo poskytujete, představuje riziko pro váš systém iSeries a pro síť, ke které je připojen. Strategie zabezpečení ochrany dat je sada pravidel, která se používají u činností týkajících se počítačových a komunikačních prostředků organizace. Tato pravidla se týkají oblastí, jako je například fyzické zabezpečení, zabezpečení dat zaměstnanců, zabezpečení administrativních dat a zabezpečení sítě.

**Strategie zabezpečení ochrany dat** definuje to, co chcete ochránit a to, co očekáváte od uživatelů vašeho systému. Je základem plánu pro zabezpečení ochrany dat při navrhování nových aplikací nebo rozšiřování vaší stávající sítě. Popisuje odpovědnost uživatelů, jako například ochranu důvěrných informací a vytváření složitých hesel. Vaše strategie zabezpečení ochrany dat by měla také popsat, jak budete efektivitu bezpečnostních opatření monitorovat. Takové monitorování vám pomůže určit, zda se někdo pokouší vaše zabezpečení obejít.

Při vyvíjení strategie zabezpečení ochrany dat musíte jasně definovat její cíle. Jakmile ji vytvoříte, musíte podniknout kroky, kterými se v ní obsažená pravidla budou realizovat. Mezi ně patří školení zaměstnanců a a dodání softwaru a hardwaru, s jejichž pomocí se pravidla uplatní. Když provádíte změny v počítačovém prostředí, měli byste také aktualizovat strategii zabezpečení ochrany dat. Tak zajistíte, že postihnete případná nová rizika, která z těchto změn vyplynou. Pod tématem ″Základní zabezpečení a plánování systému″ v rámci aplikace IBM Systems Software Information Center najdete příklad strategie zabezpečení ochrany dat společnosti JKL Toy.

## Úkoly vašeho zabezpečení ochrany dat

Když vytváříte a realizujete strategii zabezpečení ochrany dat, musíte mít jasný cíl. Úkoly zabezpečení ochrany dat spadají do jedné nebo více z těchto kategorií:

**ochrana prostředků**
Plán ochrany prostředků zajistí, aby přístup k objektům v systému měli pouze oprávnění uživatelé. Schopnost

zabezpečit všechny typy systémových prostředků je silnou stránkou serveru iSeries. Měli byste pečlivě definovat různé kategorie uživatelů, kteří mohou mít přístup do vašeho systému. Rovněž byste měli definovat, jaká přístupová oprávnění chcete dát těmto skupinám uživatelů jako součást strategie zabezpečení ochrany dat.

**autentizace**
Zabezpečení nebo ověření, že prostředek (člověk nebo systém) na druhém konci relace je skutečně tím, zač se vydává. Plné prokázání pravosti brání systém proti riziku, kdy se odesílatel nebo přijímající vydává za někoho jiného a používá falešnou identitu, aby získal přístup k systému. Tradičně používaly systémy pro autentizaci heslo a jméno uživatele; digitální certifikáty mohou nabídnout bezpečnější metodu autentizace a přitom poskytují pro zabezpečení ještě další výhody. Když připojíte systém k veřejné síti jakou je Internet, nabývá autentizace uživatele nových rozměrů. Důležitý rozdíl Internetem a vnitropodnikovou sítí (intranet) je vaše schopnost důvěřovat identitě uživatele, který se do systému přihlásí. V důsledku toho byste měli vážně uvažovat o použití účinnějších metod autentizace, než nabízejí tradiční procedury přihlášení pomocí hesla a jména uživatele. Ověření uživatelé mohou mít různé typy povolení, která se zakládají na úrovni jejich oprávnění.

**oprávnění**
Zabezpečení, aby osoba nebo počítač na druhém konci relace měla povolení provést požadavek. Oprávnění je proces určení, kdo nebo co může mít přístup k systémovým prostředkům nebo provádět v systému jisté činnosti. Kontrola oprávnění se obvykle provádí v kontextu autentizace.

**integrita**
Zabezpečení toho, aby přicházející informace byly stejné jako odesílané. Chcete-li pochopit integritu, musíte porozumět pojmům integrita dat a integrita systému.

- **Integrita dat**: Data jsou chráněna před neoprávněnými změnami nebo zfalšováním. Integrita dat chrání před bezpečnostním rizikem manipulace, kdy někdo zachytí a změní informace, ke kterým nemá oprávnění. Kromě ochrany dat uložených ve vaší síti budete možná potřebovat další zabezpečení dat, abyste zajistili integritu dat vstupujících do vašeho systému z nedůvěryhodných zdrojů. Když do vašeho systému vstupují data z veřejné sítě, budete potřebovat metody zabezpečení dat, abyste mohli udělat dále uvedené akce:
  - Ochránit data před “čmuchánim” a interpretací, obvykle jejich zašifrováním.
  - Zajistit, aby přenos nebyl pozměněn (integrita dat).
  - Prokázat, že k přenosu došlo (neodmítání). V budoucnosti budete možná potřebovat elektronický ekvivalent doporučené nebo úředně kontrolované pošty.
- **Integrita systému**: Váš systém poskytuje konzistentní, očekávané výsledky při očekávaném výkonu. U serveru iSeries je integrita systému nejčastěji přehlíženou komponentou zabezpečení ochrany dat, protože je základní součástí architektury serveru iSeries. Architektura serveru iSeries například vetřelcům nesmírně ztěžuje imitování nebo změnu programu operačního systému, pokud používáte úroveň zabezpečení 40 nebo 50.

**neodmítání**
Neodmítání je důkazem toho, že transakce proběhla nebo že jste odeslali nebo přijali zprávu. Použití digitálních certifikátů a šifrování pomocí veřejného klíče k ″podpisu″ transakcí, zpráv a dokumentů podporuje neodmítání. Odesílatel i příjemce souhlasí, že k výměně došlo. Digitální podpis u dat poskytuje nezbytný důkaz.

**důvěrnost**
Zabezpečení, aby citlivé informace zůstaly soukromé a nebyly viditelné slídilům. Důvěrnost je nanejvýš důležitá pro celkové zabezpečení dat. Zašifrování dat pomocí digitálních certifikátů a protokolu SSL (Secure Sockets Layer) pomůže zajistit důvěrnost při přenosu dat přes nedůvěryhodné sítě. Strategie zabezpečení ochrany dat by se měla zabývat tím, jak zajistit důvěrnost informací nejen ve vaší síti, ale také v okamžiku, kdy vaši síť opustí.

**prověřování zabezpečovacích aktivit**
Monitorování událostí důležitých pro zabezpečení do protokolu úspěšných i neúspěšných (odepřených) přístupů. Záznamy o úspěšném přístupu vám řeknou, kdo co ve vašich systémech dělá. Záznamy o neúspěšném přístupu vám řeknou buď to, že se někdo pokouší porušit vaše zabezpečení dat, nebo že má někdo potíže s přístupem do vašeho systému.

Pochopení cílů zabezpečení ochrany dat vám pomůže vytvořit strategii zabezpečení ochrany dat, která pokryje všechny potřeby zabezpečení ochrany dat ve vaší síti i v síti Internet. Při definování vašich cílů a vytváření strategie zabezpečení ochrany dat vás může inspirovat téma Scénář: Plán elektronického podnikání firmy JKL Toy. Využití Internetu a plán zabezpečení ochrany dat společnosti ve scénáři je reprezentativní pro mnoho implementací z reálného světa.

**Související pojmy**

“Faktory zabezpečení systému iSeries a Internetu” na stránce 2
Zde naleznete přehled silných stránek zabezpečení ochrany dat systému iSeries a nabídky zabezpečení ochrany dat.

“Metoda zabezpečení ochrany dat pomocí vrstvené obrany” na stránce 4
**Strategie zabezpečení ochrany dat** definuje to, co chcete ochránit a to, co očekáváte od uživatelů vašeho systému.

Digitální certifikáty

Secure Socket Layer (SSL)

“Scénář: Plán elektronického podnikání firmy JKL Toy Company”
Popisuje typickou firmu se jménem JKL Toy, která se rozhodla rozšířit své obchodní záměry používáním sítě Internet. I když jde o fiktivní společnost, jsou její plány na využití sítě Internet pro elektronické podnikání a z toho vyplývající potřeby zabezpečení ochrany dat reprezentativní pro situaci mnoha firem v reálném světě.

## Scénář: Plán elektronického podnikání firmy JKL Toy Company

Popisuje typickou firmu se jménem JKL Toy, která se rozhodla rozšířit své obchodní záměry používáním sítě Internet. I když jde o fiktivní společnost, jsou její plány na využití sítě Internet pro elektronické podnikání a z toho vyplývající potřeby zabezpečení ochrany dat reprezentativní pro situaci mnoha firem v reálném světě.

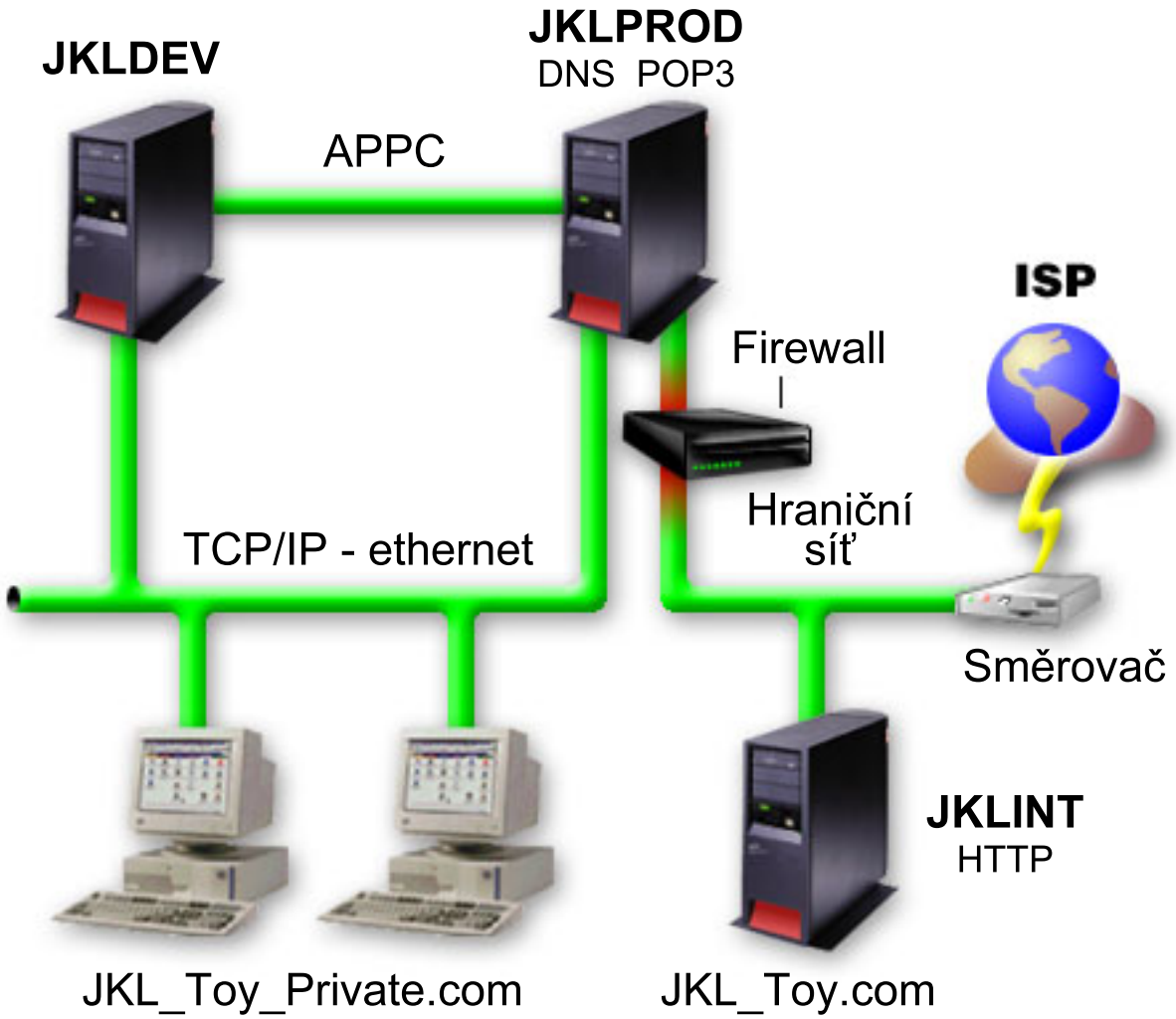
Firma JKL Toy je malý, ale rychle rostoucí výrobce hraček od švihadel, přes draky až po vycpané leopardy na hraní. Prezident společnosti je nadšený růstem obchodu a tím, jak jeho nový systém iSeries snižuje zátěž, která s tímto růstem souvisí. Sharon Jonesová, vedoucí účtárny, je zodpovědná za administraci systému iSeries a za jeho zabezpečení.

Firma JKL Toy úspěšně používá svou strategii zabezpečení ochrany dat interních aplikaci již více než rok. Nyní má v plánu instalovat intranet (vnitropodnikovou síť) s cílem efektivnějšího sdílení interních informací. Firma má také v plánu začít s využitím sítě Internet na podporu svých obchodních cílů. Patří mezi ně plány na vytvoření společné marketingové účasti v síti Internet, včetně online katalogu. Chtějí také používat Internet k přenosu citlivých informací ze vzdálených počítačů do společné kanceláře. Kromě toho chce firma umožnit zaměstnancům ve vývojové laboratoři přístup k síti Internet za účelem výzkumu a vývoje. A konečně chce firma umožnit, aby zákazníci používali její webovou stránku pro přímé online nákupy. Sharon pracuje na zprávě o specifických potenciálních rizicích těchto aktivit a o tom, jaká bezpečnostní opatření by měla firma podniknout, aby tato rizika minimalizovala. Sharon bude zodpovědná za aktualizaci strategie zabezpečení ochrany dat a za realizaci bezpečnostních opatření, která má firma v úmyslu použít.

Zvýšená přítomnost v síti Internet má tyto cíle:

- Propagovat obecný obraz a přítomnost společnosti jako součást marketingové kampaně.
- Poskytnout zákazníkům a pracovníkům prodeje online katalog produktů.
- Zlepšit služby zákazníkům.
- Poskytnout zaměstnancům elektronickou poštu a přístup do sítě World Wide Web.

Poté, co firma JKL Toy zajistila výrazné základní zabezpečení svých serverů iSeries, rozhodla se zakoupit a používat produkt ochranné bariéry, který má zabezpečit ochranu na úrovni sítě. Ochranná bariéra ochrání její interní síť před rizikem spojeným s používáním sítě Internet. Zde vidíte ilustraci konfigurace sítě Internet uvedené firmy.




Na diagramu vidíte, že firma JKL Toy má dva primární servery iSeries. Jeden systém používá pro aplikace vývoje (JKLDEV) a druhý pro výrobní aplikace (JKLPROD). Oba systémy pracují s životně důležitými daty a aplikacemi. V důsledku toho firmě příliš nevyhovuje spouštět v těchto systémech internetové aplikace. Místo toho se rozhodla přidat nový server iSeries (JKLINT), kde se takové aplikace budou spouštět.

Společnost umístila nový systém do hraniční sítě a používá ochrannou bariéru mezi ní a svou hlavní interní sítí, aby zajistila lepší oddělování mezi vlastní sítí a sítí Internet. Takové oddělení snižuje riziko plynoucí z používání Internetu, vůči kterému jsou interní systémy zranitelné. Vymezením nového serveru iSeries jako výlučně internetového serveru snižuje firma také složitost správy zabezpečení své sítě.

Současně nebude firma na novém serveru iSeries provozovat žádné životně důležité aplikace. V této etapě plánování elektronického podnikání bude systém poskytovat pouze statickou veřejnou webovou stránku. Firma však chce implementovat bezpečnostní opatření na ochranu systému a veřejných webových stránek, které provozuje, aby zabránila přerušení služeb a jiným možným útokům. V důsledku toho bude firma chránit systém pravidly pro filtrování paketu a pro převod síťových adres (NAT), stejně jako výraznými základními bezpečnostními opatřeními.

Až firma vyvine pokročilejší veřejné aplikace (jako například webovou stránku pro elektronický obchod nebo pro přístup k síti extranet), bude implementovat i rozsáhlejší bezpečnostní opatření.

**Související pojmy**

"Strategie a cíle zabezpečení ochrany dat" na stránce 6
Definice, co se má chránit, a co lze očekávat od uživatelů.

"Volby zabezpečení sítě" na stránce 11
Popisuje bezpečnostní opatření, o jejichž implementaci na úrovni sítě byste měli uvažovat, chcete-li zajistit ochranu vašich interních prostředků.

"Volby zabezpečení přenosu dat" na stránce 23
Obsahuje informace o bezpečnostních opatřeních, která můžete aplikovat při ochraně dat, když procházejí přes nedůvěryhodné sítě, jako je například Internet. K těmto opatřením patří připojení pomocí protokolu SSL (Secure Sockets Layer), produkt iSeries Access Express a připojení VPN (Virtual Private Network).

## Úrovně zabezpečení systému v rámci základní přípravy na připojení k Internetu

Popisuje, jaké zabezpečení systému byste měli mít předtím, než se připojíte k Internetu.

Opatření pro zabezpečení systému představují poslední obrannou linii proti problémům s bezpečností v síti Internet. V důsledku toho musí být vaším prvním krokem v celkové strategii zabezpečení Internetu řádná konfigurace základních nastavení zabezpečení systému i5/OS. Chcete-li zajistit, aby zabezpečení vašeho systému odpovídalo minimálním požadavkům, postupujte takto:

- Nastavte úroveň zabezpečení (systémová hodnota QSECURITY) na 50. Úroveň zabezpečení 50 poskytuje nejvyšší úroveň ochrany integrity, což se velmi doporučuje pro ochranu systému v prostředí s vysokým rizikem, jakým je například síť Internet. Podrobnější informace o jednotlivých úrovních zabezpečení serveru iSeries najdete v publikaci Plánování a nastavení zabezpečení systému.

  **Poznámka:** Jestliže v současné době pracujete na nižší úrovni zabezpečení než 50, budete muset aktualizovat buď obslužné procedury, nebo vlastní aplikace. Měli byste si prostudovat informace uvedené v publikaci iSeries Zabezpečení - referenční informace, než změníte úroveň zabezpečení na vyšší úroveň.
- Nastavte systémové hodnoty, které jsou důležité pro zabezpečení, aby vyjadřovaly alespoň taková omezení, jako doporučená nastavení. Při konfiguraci doporučených bezpečnostních nastavení můžete použít program iSeries Navigator Security Wizard.
- Zajistěte, aby žádné uživatelské profily, včetně profilů dodaných od IBM, neměly předvolená hesla. Příkazem ANZDFTPWD (Analyze Default Passwords) zkontrolujete, zda máte předvolená hesla.
- K ochraně důležitých systémových prostředků použijte oprávnění k objektu. Použijte restriktivní přístup k vašemu systému. To znamená, standardně omezte všem přístup (PUBLIC *EXCLUDE) k systémovým prostředkům, jako jsou například knihovny a adresáře. Přístup k těmto vyhrazeným prostředkům povolte jen několika uživatelům. Omezení přístupu pomocí menu v prostředí sítě Internet nestačí.
- V systému **musíte** nastavit oprávnění k objektu. .

Konfiguraci těchto minimálních požadavků na zabezpečení systému vám může usnadnit buď pomocný program **Security Planner** (který je dostupný na webových stránkách IBM Systems Software Information Center), nebo program **Security Wizard** (který je dostupný prostřednictvím rozhraní produktu iSeries Navigator). Security Planner vám poskytne mnohá doporučení k zabezpečení dat na základě vašich odpovědí na řadu otázek. Tato doporučení můžete použít při konfiguraci těch nastavení zabezpečení systému, která potřebujete. Průvodce Security Wizard také poskytuje doporučení na základě vašich odpovědí na řadu otázek. Na rozdíl od pomocného programu Security Advisor můžete průvodce použít k tomu, aby nastavení zabezpečení systému nakonfiguroval za vás.

Inherentní funkce zabezpečení dat serveru iSeries, jsou-li správně nakonfigurovány a spravovány, vám poskytnou možnost minimalizovat mnohá rizika. Když však připojíte váš server iSeries k síti Internet, budete muset učinit další bezpečnostní opatření, aby byla zajištěna bezpečnost vaší interní sítě. Poté, co zajistíte, aby váš server iSeries měl dobré všeobecné zabezpečení systému, jste připraveni konfigurovat další bezpečnostní opatření jako součást vašeho celkového plánu zabezpečení využití Internetu.

**Související pojmy**

"Metoda zabezpečení ochrany dat pomocí vrstvené obrany" na stránce 4
**Strategie zabezpečení ochrany dat** definuje to, co chcete ochránit a to, co očekáváte od uživatelů vašeho systému.

**Související informace**

# Volby zabezpečení sítě

Popisuje bezpečnostní opatření, o jejichž implementaci na úrovni sítě byste měli uvažovat, chcete-li zajistit ochranu vašich interních prostředků.

Když se připojujete k nedůvěryhodné síti, vaše strategie zabezpečení ochrany dat musí zahrnovat úplné schéma zabezpečení ochrany dat, včetně bezpečnostních opatření, která budete implementovat na úrovni sítě. Instalace ochranné bariéry je nejlepším prostředkem pro rozmístění vyčerpávajících bezpečnostních opatření.

Také poskytovatel služeb sítě Internet může a měl by představovat důležitý prvek v plánu zabezpečení vaší sítě. Schéma zabezpečení vaší sítě by mělo vymezit, jaká bezpečnostní opatření zajistí poskytovatel služeb sítě Internet (ISP), jako například filtrovací pravidla pro připojení směrovače ISP a opatření pro služby jmen domény (DNS).

I když ochranná bariéra představuje ve vašem celkovém plánu jednu z hlavních obranných linií, neměla by zůstat **jedinou** linií obrany. Protože se potenciální rizika zabezpečení Internetu mohou vyskytnout na nejrůznějších úrovních, musíte podniknout taková bezpečnostní opatření, která zabezpečí proti riziku více obranných vrstev.

Ochranná bariéra sice představuje obrovské zabezpečení proti určitým typům napadení, je však jen jednou součástí celkového řešení vaší bezpečnosti. Ochranná bariéra nemusí například vždy ochránit data, která odesíláte přes Internet pomocí takových aplikací, jako je například pošta SMTP, FTP a TELNET. Pokud se nerozhodnete tato data zašifrovat, může k nim kdokoliv získat přístup, když putují Internetem na místo určení.

O použití některého produktu ochranné bariéry jako hlavního nástroje ochrany byste měli vážně uvažovat, kdykoli budete připojovat server iSeries nebo vaši interní síť k Internetu. Ačkoliv již není možné zakoupit produkt IBM Firewall for AS/400 a ani podpora tohoto produktu již není k dispozici, existuje mnoho jiných produktů, které můžete používat. Podrobné scénáře týkající se různých voleb migrace popisuje téma Vše, co potřebujete vědět při migraci z IBM Firewall for AS/400.

Vzhledem k tomu, že komerční produkty ochranných bariér poskytují celé spektrum technologií pro zabezpečení sítě, firma JKL Toy si vybrala jednu z nich pro svůj scénář zabezpečení elektronického podnikání, aby nastavila ochranu své sítě. Zvolená ochranná bariéra však neposkytuje žádnou ochranu nového internetového serveru iSeries. Proto se firma rozhodla implementovat funkci Pravidla paketu iSeries, pomocí které vytvoří filtry a pravidla NAT pro řízení provozu na internetovém serveru.

## Pravidla paketu systému iSeries

Pravidla pro filtrování paketu umožňují nastavit ochranu počítačových systémů odmítnutím nebo přijetím IP paketů podle kritérií, která definujete. Pravidla pro převod síťových adres (NAT) vám umožní skrýt interní systémové informace před externími uživateli nahrazením jedné IP adresy jinou, veřejnou IP adresou. Přestože pravidla pro filtry IP paketu a NAT představují jádro technologií pro zabezpečení sítě, neposkytují stejnou úroveň zabezpečení jako plně funkční ochranná bariéra (firewall). Při rozhodování mezi kompletním produktem ochranné bariéry a funkcí pravidel paketu systému iSeries byste měli pečlivě analyzovat požadavky a cíle svého zabezpečení dat.

Téma Výběr voleb pro zabezpečení sítě iSeries vám pomůže rozhodnout, který přístup odpovídá potřebám vašeho zabezpečení ochrany dat.

**Související pojmy**

“Metoda zabezpečení ochrany dat pomocí vrstvené obrany” na stránce 4
**Strategie zabezpečení ochrany dat** definuje to, co chcete ochránit a to, co očekáváte od uživatelů vašeho systému.

“Scénář: Plán elektronického podnikání firmy JKL Toy Company” na stránce 8
Popisuje typickou firmu se jménem JKL Toy, která se rozhodla rozšířit své obchodní záměry používáním sítě Internet. I když jde o fiktivní společnost, jsou její plány na využití sítě Internet pro elektronické podnikání a z toho vyplývající potřeby zabezpečení ochrany dat reprezentativní pro situaci mnoha firem v reálném světě.

“Pravidla paketu systému iSeries” na stránce 13
Pravidla paketu systému iSeries je integrovaná funkce systému i5/OS dostupná z prostředí produktu iSeries Navigator.

“Výběr voleb zabezpečení sítě iSeries” na stránce 15
Obsahuje stručné informace o tom, jaké volby zabezpečení ochrany dat byste měli zvolit na základě svých plánů na využití sítě Internet.

**Související informace**

Vše, co potřebujete vědět při migraci z IBM Firewall for AS/400

# Ochranná bariéra

Ochranná bariéra je blokáda mezi zabezpečenou sítí a nedůvěryhodnou sítí, jakou je například Internet.

Většina firem používá k bezpečnému připojení interní sítě k Internetu ochrannou bariéru, i když ji lze použít také k zabezpečení jedné interní sítě před druhou.

Ochranná bariéra poskytuje jediný řízený bod kontaktu mezi vaší zabezpečenou interní sítí a nedůvěryhodnou sítí, nazývaný jako ″chokepoint″. Ochranná bariéra:

- Dovoluje uživatelům vaší interní sítě používat povolené prostředky nacházející se ve vnější síti.
- Zabraňuje neoprávněným uživatelům z vnější sítě používat prostředky ve vaší interní síti.

Když používáte ochrannou bariéru jako bránu do sítě Internet (nebo do jiné sítě), podstatně snižujete riziko hrozící interní síti. Použití ochranné bariéry usnadňuje i správu zabezpečení sítě, protože její funkce provádějí mnoho direktiv vaší strategie zabezpečení ochrany dat.

## Jak pracuje ochranná bariéra

Chcete-li pochopit, jak ochranná bariéra funguje, představte si, že vaše síť je budova a vy řídíte přístup do ní. Budova má halu jako jediný vstupní bod. V této hale jsou recepční, kteří hosty vítají, bezpečnostní služba, která na ně dává pozor, videokamery pro zaznamenání jejich chování a čtecí zařízení pro propustky, a ti všichni prověřují návštěvníky vstupující do budovy.

Tato opatření mohou dobře fungovat při kontrole přístupu do budovy. Když se ale neoprávněné osobě podaří do ní vstoupit, neexistuje způsob, jak budovu před jednáním vetřelce ochránit. Jestliže však budete jeho pohyb monitorovat, máte šanci případné podezřelé jednání vetřelce odhalit.

## Komponenty ochranné bariéry

Ochranná bariéra je kolekce hardwaru a softwaru, které, jsou-li použity společně, zabraňují neoprávněnému přístupu do části sítě. Bariéra se skládá z následujících komponent:

- Hardware. Hardware ochranné bariéry obvykle tvoří samostatný počítač nebo zařízení vyhrazené k provádění softwarových funkcí ochranné bariéry.
- Software. Software ochranné bariéry nabízí celou řadu aplikací. V kontextu zabezpečení sítě poskytuje ochranná bariéra prostřednictvím různých technologií tyto bezpečnostní kontroly:
  - IP pakety, filtrování.
  - Služby NAT (převod síťových adres).
  - Server SOCKS.
  - Proxy servery pro nejrůznější služby, jako například HTTP, Telnet, FTP, atd.
  - Služby přenosu pošty.
  - Rozdělení - DNS.
  - Protokolování.
  - Monitorování v reálném čase.

**Poznámka:** Některé ochranné bariéry poskytují služby VPN, takže můžete nastavit zašifrované relace mezi vaší ochrannou bariérou a jinými kompatibilními bariérami.

### Použití technologií ochranné bariéry

Pomocí proxy serverů, serveru SOCKS nebo pravidel NAT ochranné bariéry můžete interním uživatelům poskytnout bezpečný přístup k službám sítě Internet. Proxy server a server SOCKS přeruší spojení TCP/IP u ochranné bariéry, aby skryly síťové informace před nedůvěryhodnou sítí. Servery také poskytují další možnosti protokolování.

Pomocí NAT můžete uživatelům Internetu poskytnout snadný přístup k veřejnému serveru za ochrannou bariérou. Ochranná bariéra přesto vaši síť ochrání, protože NAT skryje interní IP adresy.

Ochranná bariéra může také ochránit interní informace tím, že poskytne server DNS, který může sama používat. Ve skutečnosti máte dva servery DNS: jeden používáte pro data o interní síti a druhý je v ochranné bariéře pro data o externích sítích a o samotné bariéře. To vám umožňuje řídit vnější přístup k informacím o vašich interních systémech.

Když definujete strategii vaší ochranné bariéry, můžete se domnívat, že postačí zakázat všechno, co představuje riziko pro organizaci, a všechno ostatní povolit. Počítačoví zločinci však neustále vytvářejí nové metody napadení, a proto musíte předvídat, jak takovým útokům předejít. Jako v příkladu o budově budete také muset sledovat, zda někdo nějakým způsobem nenapadl vaši obranu. Obecně řečeno je mnohem nákladnější zotavit se ze škod z napadení systému, než útoku předejít.

V případě ochranné bariéry je nejlepší strategií povolit pouze ty aplikace, které jste otestovali a kterým důvěřujete. Budete-li se držet této strategie, musíte vyčerpávajícím způsobem definovat seznam služeb, které ochranná bariéra musí poskytovat. Každou službu můžete charakterizovat směrem spojení (zevnitř ven nebo zvenčí dovnitř). Měli byste také vytvořit seznam uživatelů, kterým poskytnete oprávnění k používání jednotlivých služeb a počítače, které mohou zajistit připojení pro tyto služby.

### Jak může ochranná bariéra ochránit vaši síť

Ochrannou bariéru instalujete mezi vaši síť a bod připojení k Internetu (nebo jiné nedůvěryhodné síti). Bariéra pak umožňuje, abyste omezili vstupní body do vaší sítě. Ochranná bariéra poskytuje jediný styčný bod mezi vaší sítí a sítí Internet, nazývaný chokepoint. Protože máte jediný styčný bod, máte větší kontrolu nad tím, jakému provozu povolíte vstup do sítě a výstup z ní.

Ochranná bariéra se veřejnosti jeví jako jediná adresa. Poskytuje přístup do nedůvěryhodné sítě přes proxy server, server SOCKS nebo službu NAT (převod síťových adres) a přitom skryje interní síťové adresy. V důsledku toho udržuje ochranná bariéra soukromí vaší interní sítě. To, že ochranná bariéra udržuje informace o vaší síti jako soukromé, představuje jeden ze způsobů ochrany, jež činí útok pomocí vydávání se za někoho jiného (tzv. spoofing) méně pravděpodobným.

Ochranná bariéra vám umožňuje řídit provoz do a ze sítě a minimalizovat tak riziko jejího napadení. Bezpečně filtruje veškerý provoz, který vstupuje do vaší sítě tak, že mohou vstoupit jen určité typy provozu pro určitá místa určení. To minimalizuje riziko, že by někdo mohl použít TELNET nebo protokol FTP k získání přístupu k vašim interním systémům.

### Co ochranná bariéra pro ochranu vaší sítě nemůže udělat

Ochranná bariéra sice představuje obrovské zabezpečení proti určitým typům napadení, je však jen jednou součástí celkového řešení vaší bezpečnosti. Ochranná bariéra nemusí například vždy ochránit data, která odesíláte přes Internet pomocí takových aplikací, jako je například pošta SMTP, FTP a TELNET. Pokud se nerozhodnete tato data zašifrovat, může k nim kdokoliv získat přístup, když putují Internetem na místo určení.

## Pravidla paketu systému iSeries

Pravidla paketu systému iSeries je integrovaná funkce systému i5/OS dostupná z prostředí produktu iSeries Navigator.

Funkce pravidla paketu umožňuje pro ochranu systému iSeries nakonfigurovat dvě základní technologie pro zabezpečení sítě, které řídí provoz TCP/IP:

- převod síťových adres (NAT)
- filtrování IP paketů

Protože jsou NAT a filtrování IP paketů integrální součástí systému i5/OS, nabízí úsporný způsob, jak systém zabezpečit. V některých případech mohou tyto bezpečnostní technologie obstarat všechno, co potřebujete a nemusíte nic dalšího kupovat. Tyto technologie však nevytvářejí opravdovou funkční ochrannou bariéru. Zabezpečení IP paketů můžete použít samostatně nebo ve spojení s ochrannou bariérou podle požadavků a cílů vaší ochrany.

**Poznámka:** Jestliže plánujete zabezpečení provozního systému iSeries, neměli byste se pokoušet využívat výhody úspory nákladů. V podobných situacích by mělo mít zabezpečení vašeho systému přednost před náklady. Chcete-li pro váš provozní systém zajistit maximální možnou ochranu, měli byste uvažovat o použití ochranné bariéry.

## Co je to NAT a filtrování IP paketů a jakým způsobem tyto funkce spolupracují?

**Převod síťových adres (NAT)** změní zdrojové nebo cílové IP adresy paketů, které procházejí systémem. NAT nabízí transparentnější alternativu proxy serverů a SOCKS serverů ochranné bariéry. NAT také může zjednodušit konfiguraci sítě, protože povoluje vzájemně spojit sítě s nekompatibilním členěním adresování. V důsledku toho můžete použít pravidla NAT tak, aby systém iSeries vystupoval jako brána mezi dvěma sítěmi, které mají konfliktní nebo nekompatibilní schémata adresování. NAT je také možné použít pro ukrytí skutečných IP adres jedné sítě tak, že dynamicky nahradíte jednu nebo více reálných adres. Vzhledem k tomu, že se funkce filtrování IP paketu a NAT vzájemně doplňují, budete je často používat společně za účelem lepšího zabezpečení sítě.

Použití NAT může také zjednodušit provoz veřejného webového serveru za ochrannou bariérou. Veřejné IP adresy pro webový server se převádějí na soukromé IP adresy. To snižuje počet registrovaných IP adres, které jsou zapotřebí, a minimalizuje dopad na stávající síť. Poskytuje také mechanismus, aby interní uživatelé měli přístup k Internetu a přitom skryli soukromé interní IP adresy.

**Filtrování IP paketu** nabízí schopnost selektivně zablokovat nebo ochránit provoz IP na základě informací v záhlaví paketů. K rychlému a snadnému nakonfigurování základních filtrovacích pravidel pro zablokování nežádoucího provozu v síti můžete použít průvodce Internet Setup Wizard v aplikaci iSeries Navigator.

Filtrování IP paketu můžete použít k těmto účelům:

- Vytvořit sadu filtrovacích pravidel k zadání, kterým IP paketům povolit a kterým odepřít přístup do vaší sítě. Když vytváříte filtrovací pravidla, aplikujete je na fyzické rozhraní (například Token-Ring nebo linku typu Ethernet). Pravidla můžete aplikovat na několik fyzických rozhraní nebo můžete u každého rozhraní použít jiná pravidla.
- Vytvořit pravidla, která buď povolí, nebo zamítnou specifické pakety a která jsou založena na následujících informacích záhlaví:
  - IP adresa místa určení.
  - Protokol IP adresy zdrojového systému (například TCP, UDP a tak dále).
  - Port místa určení (například HTTP má port 80).
  - Port zdroje.
  - Směr IP datagramu (příchozí nebo odchozí).
  - Směrováno nebo lokální.
- Předejít tomu, aby nežádoucí nebo zbytečný provoz dosáhl aplikací v systému. Můžete také zabránit směrování provozu do jiných systémů. To zahrnuje pakety ICMP nižší úrovně (například pakety PING), pro které není zapotřebí žádný specifický aplikační server.
- Specifikujte, zda filtrovací pravidlo vytvoří záznam v protokolu systémového žurnálu o paketech, které pravidlu odpovídají. Jakmile se informace zapíší do systémového žurnálu, nemůžete již záznam v protokolu změnit. Díky tomu je protokol ideálním nástrojem pro prověřování aktivity sítě.

**Související pojmy**

"Volby zabezpečení sítě" na stránce 11
Popisuje bezpečnostní opatření, o jejichž implementaci na úrovni sítě byste měli uvažovat, chcete-li zajistit ochranu vašich interních prostředků.

Převod síťových adres (NAT)

Filtrování IP paketů

## Výběr voleb zabezpečení sítě iSeries

Obsahuje stručné informace o tom, jaké volby zabezpečení ochrany dat byste měli zvolit na základě svých plánů na využití sítě Internet.

Řešení zabezpečení sítě, která chrání před neoprávněným přístupem, obvykle spoléhají na technologie ochranné bariéry. Chcete-li ochránit svůj systém iSeries, můžete se rozhodnout pro použití plně funkční ochranné bariéry, nebo pro specifické technologie zabezpečení sítí, které jsou součástí implementace protokolu TCP/IP v systému i5/OS. Tato implementace se skládá z funkce pravidel paketu (která zahrnuje filtrování IP a NAT) a z proxy serveru HTTP for iSeries.

Volba mezi použitím funkce pravidel paketů nebo ochranné bariéry záleží na prostředí vaší sítě, přístupových požadavcích a potřebách zabezpečení. O použití některého produktu ochranné bariéry jako hlavního nástroje ochrany byste měli **vážně** uvažovat, kdykoli budete připojovat server iSeries nebo vaši interní síť k Internetu nebo jiné nedůvěryhodné síti.

Ochranná bariéra je v tomto případě vhodnější, protože je to typicky jednoúčelové hardwarové a softwarové zařízení s omezeným počtem rozhraní pro externí přístup. Když použijete technologie TCP/IP operačního systému i5/OS pro ochranu přístupu k Internetu, používáte obecnou počítačovou platformu s nesčíslným počtem rozhraní a aplikací otevřených externímu přístupu.

Tento rozdíl je důležitý z mnoha důvodů. Produkt jednoúčelové ochranné bariéry například neposkytuje žádné další funkce ani aplikace mimo ty, které patří k samotné bariéře. Proto i kdyby vetřelec ochrannou bariéru úspěšně obešel a získal k ní přístup, nemohl by toho moc udělat. Naopak kdyby vetřelec obešel funkce zabezpečení TCP/IP na serveru iSeries, mohl by mít potenciálně přístup k různým užitečným aplikacím, službám a datům. Vetřelec je může použít a způsobit škody v samotném systému anebo získat přístup k dalším systémům ve vaší interní síti.

Je tedy vůbec někdy přijatelné použít funkce zabezpečení protokolu TCP/IP systému iSeries? Jako u každého rozhodování ve věcech ochrany, musíte svá rozhodnutí založit na poměru získaného prospěchu vůči nákladům, které jste ochotni vynaložit. Musíte analyzovat cíle svého podnikání a rozhodnout, jaké riziko jste ochotni přijmout v poměru k nákladům na to, jakým zabezpečením chcete riziko minimalizovat. Následující tabulka nabízí informace o tom, kdy je odpovídající použít funkce zabezpečení dat TCP/IP oproti plně funkčnímu zařízení firewall. Tabulku můžete použít k rozhodnutí, zda byste měli k zabezpečení sítě a ochraně systému použít firewall, funkce zabezpečení dat TCP/IP nebo kombinaci obou přístupů.

| Technologie zabezpečení ochrany dat | Nejlepší použití technologie TCP/IP systému i5/OS | Nejlepší použití plně funkční ochranné bariéry |
|---|---|---|
| Filtrování IP paketů | • Poskytnout **dodatečnou** ochranu pro jediný server iSeries, jako je např. veřejný webový server nebo intranetový systém s citlivými daty.<br>• Chránit dílčí síť společné sítě **intranet**, když server iSeries působí jako brána (příležitostný směrovač) do zbývající části sítě.<br>• Řídit komunikaci s ne zcela důvěryhodným partnerem přes **soukromou síť** nebo extranet, kde server iSeries působí jako brána. | • Chránit celou společnou síť proti síti **Internet** nebo jiné nedůvěryhodné síti, ke které je vaše síť připojena.<br>• Chránit velkou dílčí síť před hustým provozem ze zbývající části společné sítě. |

| Technologie zabezpečení ochrany dat | Nejlepší použití technologie TCP/IP systému i5/OS | Nejlepší použití plně funkční ochranné bariéry |
|---|---|---|
| NAT (převod síťových adres) | • Umožnit spojení dvou **soukromých sítí** s nekompatibilní strukturou adresování.<br>• Skrýt adresy dílčí sítě před méně důvěryhodnou sítí. | • Skrýt adresy klientů přistupujících k síti **Internet** nebo jiné nedůvěryhodné síti. Použít jako alternativu k serverům proxy a SOCKS.<br>• Zpřístupnit služby nějakého systému v soukromé síti klientům v síti **Internet**. |
| Proxy server | • Fungovat jako proxy server ve **vzdálených systémech** ve společné síti, když centrální ochranná bariéra poskytuje přístup k síti Internet. | • Fungovat jako proxy server pro celou společnou síť při přístupu k síti **Internet**. |

Další informace o používání funkcí TCP/IP systému i5/OS pro zabezpečení ochrany dat najdete v těchto zdrojích:

- Téma *Pravidla paketů (filtrování a NAT)* v rámci aplikace IBM Systems Software Information Center pro verzi V5R1.
- Webové stránky *HTTP Server Documentation Center* na této adrese URL:

  `http://www.iseries.ibm.com/domino/reports.htm`
- Červená kniha AS/400 Internet Security Scenarios: A Practical Approach (SG24-5954).

**Související pojmy**

"Volby zabezpečení sítě" na stránce 11
Popisuje bezpečnostní opatření, o jejichž implementaci na úrovni sítě byste měli uvažovat, chcete-li zajistit ochranu vašich interních prostředků.

## Volby zabezpečení aplikací

Obsahuje informace o bezpečnostních rizicích a volbách pro správu těchto rizik u řady oblíbených internetových aplikací a služeb.

Opatření pro zabezpečení na úrovni aplikace řídí, jak mohou uživatelé se specifickými aplikacemi zacházet. Obecně byste měli konfigurovat nastavení zabezpečení u každé aplikace, kterou používáte. Zvláštní péči byste však měli věnovat nastavení zabezpečení dat u těch aplikací a služeb, které budete v síti Internet využívat nebo do něj poskytovat. Takové aplikace a služby jsou citlivé na zneužití ze strany neoprávněných uživatelů hledajících způsob, jak získat přístup do systémů vaší sítě. Opatření pro zabezpečení dat, která se rozhodnete použít, musí pokrýt ohrožení jak na straně serveru, tak i na straně klienta.

I když je důležité zabezpečit každou aplikaci, kterou používáte, hrají bezpečnostní opatření malou úlohu v implementaci celkové strategie zabezpečení ochrany dat.

Další informace o tom, co byste měli udělat pro zabezpečení některých běžných aplikací v síti Internet, najdete v níže uvedených tématech:

**Související pojmy**

"Metoda zabezpečení ochrany dat pomocí vrstvené obrany" na stránce 4
**Strategie zabezpečení ochrany dat** definuje to, co chcete ochránit a to, co očekáváte od uživatelů vašeho systému.

## Zabezpečení webových služeb

Když poskytujete návštěvníkům přístup ke svým webovým stránkám, nechcete jim samozřejmě odhalovat informace o tom, jak jsou vaše stránky nastaveny a jaké kódování je použito k jejich vygenerování.

Chcete, aby pro ně byla návštěva vašich stránek snadná, rychlá a bezproblémová a aby veškerá práce byla prováděna skrytě. Jako administrátorovi vám jistě záleží na tom, aby zvolené metody zabezpečení negativně neovlivňovaly vaše webové stránky. Pokud jako webový server používáte server iSeries, vezměte v úvahu následující body:

- Než dojde k interakci mezi klientem a HTTP serverem, musí administrátor serveru definovat pro server určité směrnice. Existují dvě metody pro vytvoření bezpečnostních kontrol: všeobecné směrnice pro server a směrnice pro ochranu serveru. Každý požadavek vůči webovému serveru musí splňovat všechna omezení obsažená v těchto směrnicích. Teprve pak je serverem akceptován.
- Tyto směrnice můžete vytvářet a editovat pomocí administračních webových stránek určených pro konfigurování serveru. Směrnice pro server vám umožňují řídit veškeré chování webového serveru. Směrnice pro ochranu serveru dovolují specifikovat a řídit modely zabezpečení ochrany dat, které server používá pro specifické adresy URL, s nimiž webový server pracuje.
- Při konfiguraci serveru můžete použít směrnice typu ″map″ a směrnice typu ″pass″ a dále webové stránky pro administraci serveru.
  - Směrnice typu ″map″ a ″pass″ slouží k maskování jmen souborů na vašem webovém serveru iSeries. Konkrétně se jedná o směrnice serveru PASS a směrnice serveru MAP, které řídí adresáře, z nichž webový server obsluhuje URL. Můžete se setkat rovněž s se směrnicí serveru EXEC, která řídí knihovny, v nichž jsou uloženy programy CGI-BIN.

    Směrnice pro ochranu definujete pro každou adresu URL serveru. Ne všechny adresy URL vyžadují směrnici pro ochranu. Pokud však chcete řídit to, kdo a jak přistupuje ke zdroji adresy URL, je směrnice pro ochranu dané adresy URL nezbytná.
  - Namísto použití příkazu WRKHTTPCFG (Work with HTTP Configuration) a psaní směrnic máte také možnost použít ke konfigurování serveru webové stránky pro administraci serveru. Práce se směrnicemi pro ochranu prostřednictvím rozhraní příkazové řádky může být velmi složitá. Z toho důvodu doporučujeme, abyste raději použili administrační webové stránky a zajistili tak správné nastavení vašich směrnic.

  Protokol HTTP vám poskytuje schopnost zobrazovat data, nikoliv však možnost upravovat data v databázových souborech. Nicméně některé aplikace, které napíšete, budou vyžadovat aktualizaci databázového souboru. V takových případech se využívají programy CGI-BIN. Například budete potřebovat vytvořit formuláře a poté, co je uživatelé vyplní, jimi aktualizovat databázi iSeries. Jako administrátor systému byste měli monitorovat autorizace tohoto uživatelského profilu a funkce, které programy CGI provádějí. Také byste měli zhodnotit, které citlivé objekty by mohly mít nepřiměřené veřejné oprávnění.

  **Poznámka:** Rozhraní CGI (Common Gateway Interface) je průmyslovým standardem pro výměnu informací mezi webovým serverem a počítačovými programy, které jsou vůči němu externí. Programy mohou být napsány v libovolném programovacím jazyce, který je podporován operačním systémem, pod nímž se webový server spouští.

  Kromě programů CGI můžete chtít na svých webových stránkách používat také programovací jazyk Java. S problematikou zabezpečení dat v Javě byste měli být obeznámeni dříve, než přidáte Javu do svých webových stránek.

  HTTP server poskytuje protokol přístupů, který můžete využít k monitorování jak přístupů, tak pokusů o přístup prostřednictvím serveru.

  Proxy server přijímá požadavky HTTP z prohlížečů WWW a přeposílá je webovým serverům. Webové servery, které tyto požadavky přijímají, znají pouze IP adresu proxy serveru. Nemohou zjistit jména nebo adresy těch PC, od nichž požadavky vzešly. Proxy server může pracovat s požadavky URL pro HTTP, FTP (File Transfer Protocol), Gopher a WAIS.

  Za účelem konsolidace webových přístupů můžete rovněž použít podporu HTTP proxy, kterou poskytuje server IBM HTTP Server for iSeries. Proxy server může také zaznamenávat všechny požadavky URL, které slouží pro účely sledování. Vzniklé protokoly vám pak pomohou monitorovat používání a nesprávné používání (zneužívání) síťových prostředků. Další informace o použití HTTP proxy serveru můžete najít na webových stránkách IBM HTTP Server for iSeries Documentation Center na této URL adrese:

| `http://www.ibm.com/eserver/iseries/products/http/docs/doc.htm`

**Související pojmy**

“Java a zabezpečení Internetu” na stránce 18
Programování v Javě je v současném světě počítačového zpracování stále rozšířenější.

# Java a zabezpečení Internetu

Programování v Javě je v současném světě počítačového zpracování stále rozšířenější.

Můžete například používat aplikaci IBM Toolbox for Java nebo IBM Development Kit for Java na vašem systému k vývoji nových aplikací. Proto byste měli být připraveni zabývat se bezpečnostními otázkami, které s Javou souvisí. Ačkoliv ochranná bariéra představuje dobrou ochranu před nejběžnějšími bezpečnostními riziky Internetu, nezajišťuje ochranu proti řadě rizik, které s sebou používání jazyka Java přináší. Vaše strategie zabezpečení ochrany dat by měla zahrnovat podrobné zpracování ochrany systému ve třech oblastech Javy: aplikace, applety a servlety. Také byste si měli ujasnit, jakým způsobem probíhá interakce mezi Javou a zabezpečením ochrany dat na úrovni objektů ve smyslu autentizace a autorizace u programů v Javě.

## Aplikace v Javě

Jako programovací jazyk má Java některé charakteristiky, které zabraňují programátorům jazyka Java dělat neúmyslné chyby, jež by mohly vést k problémům s integritou. (Ostatní jazyky běžně používané pro PC aplikace, jako jsou např. C nebo C++, nechrání programátory před bezděčnými chybami v takové míře jako Java.) Java například používá ″strong typing″, díky němuž je programátorovi znemožněno používat objekty nezamýšleným způsobem. Java nedovoluje práci s ukazateli, v důsledku čehož programátor nemůže nechtěně přesáhnout hranice paměti daného programu. Z hlediska vývoje aplikací lze na Javu pohlížet jako na jakýkoliv vyšší programovací jazyk. Při návrhu aplikací byste měli používat stejná pravidla pro zabezpečení ochrany dat, jaká používáte u ostatních programovacích jazyků na serveru iSeries.

## Java applety

Java applety jsou malé javovské programy, které můžete zahrnout do svých HTML stránek. Jelikož jsou applety prováděny na klientovi, jde to, co tyto applety učiní, na vrub klienta. Avšak Java applet má jisté možnosti přístupu k vašemu serveru iSeries. (Rovněž program ODBC nebo komunikace APPC (advanced program-to-program communication) spouštěné na nějakém PC ve vaší síti může mít přístup do vašeho systému iSeries.) Obecně řečeno mohou Java applety vytvořit relaci pouze se serverem, z něhož byly spuštěny. Z tohoto důvodu může mít Java applet přístup do vašeho systému iSeries z PC pouze tehdy, když pochází z vašeho serveru iSeries (jako např. z webového serveru).

| Applet se může pokusit připojit k libovolnému portu TCP/IP na serveru. Nemusí nutně komunikovat se softwarovým
| serverem, který je napsán v jazyce Java. Avšak v případě serverů napsaných pomocí aplikace IBM Toolbox for Java
| musí applet poskytnout ID a heslo uživatele, chce-li vytvořit připojení zpět do serveru. Všechny servery popsané v
| tomto materiálu jsou servery iSeries. (Server napsaný v jazyce Java nemusí používat aplikaci IBM Toolbox for Java).
| Třída IBM Toolbox for Java obyčejně vyzývá uživatele k zadání ID a hesla uživatele při prvním připojení.

Applet může provádět funkce na serveru iSeries pouze za předpokladu, že je uživatelský profil pro tyto funkce autorizován. Proto se dobré schéma zabezpečení dat na úrovni prostředků stává nezbytností, pokud k zajištění nových funkcí aplikace začínáte používat Java applety. Když systém zpracovává požadavky pro applety, nepoužívá hodnotu omezených schopností v profilu daného uživatele.

Prohlížeč appletů vám umožní testovat applet v systému serveru. Applet však není předmětem bezpečnostních omezení prohlížeče. Z toho důvodu byste měli prohlížeč appletů používat pouze k testování vašich vlastních appletů, v žádném případě ke spouštění appletů z cizích zdrojů. Java applety často zapisují na pevný disk PC uživatele a dostávají tak příležitost provádět destruktivní činnost. Vy však můžete použít digitální certifikát a s jeho pomocí Java applet podepsat, což mu vytvoří autenticitu. Podepsaný applet může zapisovat na lokální jednotky PC, třebaže to předvolené nastavení prohlížeče nedovoluje. Podepsaný applet může rovněž zapisovat na mapované jednotky na vašem serveru iSeries, protože se vůči PC jeví jako lokální jednotky.

**Poznámka:** Výše popisované chování je obecně platné pro Netscape Navigator a MS Internet Explorer. To, co se děje ve skutečnosti, závisí na tom, jak máte nakonfigurovány a spravovány vámi používané prohlížeče.

U Java appletů, které pochází z vašeho serveru iSeries, budete možná potřebovat používat podepsané applety. Přesto byste měli instruovat své uživatele, aby běžně nepřijímali podepsané applety z neznámých zdrojů.

Počínaje verzí V4R4 můžete používat aplikaci IBM Toolbox for Java k nastavení prostředí SSL (Secure Sockets Layer). Můžete také použít aplikaci IBM Developer Toolkit for Java a zabezpečit aplikaci napsanou v jazyce Java pomocí SSL. Použití SSL s vašimi aplikacemi v Javě zajišťuje kódování dat včetně ID a hesel uživatelů, která se předávají mezi klientem a serverem. Pomocí produktu Digital Certificate Manager můžete nakonfigurovat registrované programy v jazyce Java tak, aby používaly protokol SSL.

## Java servlety

Servlety představují komponenty na straně serveru, které jsou napsány v jazyce Java a které dynamicky rozšiřují funkčnost webového serveru, aniž by bylo nutné měnit kód webového serveru. Server IBM WebSphere Application Server, jenž je dodáván spolu se serverem IBM HTTP Server for iSeries, poskytuje podporu pro používání servletů v systémech iSeries.

U servletů, s nimiž systém pracuje, musíte použít zabezpečení ochrany dat na úrovni prostředků. I když však na servlet aplikujete zabezpečení dat na úrovni prostředků, není jeho ochrana dostačující. Když webový server stáhne servlet, nezabrání zabezpečení dat na úrovni prostředků tomu, aby tento servlet spouštěli i ostatní. Z toho vyplývá, že byste měli zabezpečení dat na úrovni prostředků používat ve spojení s ovládacími prvky a směrnicemi pro zabezpečení HTTP serveru. Například nedovolte, aby byly servlety spouštěny pouze pod profilem webového serveru. Kromě toho byste měli řídit, kdo může spouštět servlet (maskovat klíčová slova ve směrnici pro ochranu), a to prostřednictvím skupin a přístupových seznamů (ACL) HTTP serveru. Také byste měli využívat funkcí zabezpečení ochrany dat poskytovaných vašimi nástroji pro vývoj servletů, jako jsou např. funkce v aplikaci WebSphere Application Server for iSeries.

V následujících tématech aplikace IBM Systems Software Information Center najdete podrobnější informace o obecných bezpečnostních opatřeních pro jazyk Java.

- Zabezpečení jazyka Java pro aplikaci *IBM Developer Kit for Java*.
- Třídy zabezpečení pro aplikaci *IBM Toolbox for Java*.

## Autentizace a autorizace jazyka Java vůči prostředkům

Aplikace IBM Toolbox for Java obsahuje třídy zabezpečení sloužící k ověření totožnosti uživatele a k volitelnému přiřazení této totožnosti k vláknu operačního systému pro aplikaci nebo servlet spuštěný v systému iSeries. Následné kontroly zabezpečení dat na úrovni prostředků pak probíhají pod touto přiřazenou identitou. Podrobné informace o těchto třídách zabezpečení najdete v tématu Autentizační služby produktu IBM Toolbox for Java v aplikaci IBM Systems Software Information Center.

Aplikace IBM Developer Kit for Java poskytuje podporu pro službu Java Authentication and Authorization Service (JAAS), která je standardním rozšířením produktu Java 2 Software Development Kit (J2SDK), Standard Edition. V současné době produkt J2SDK zajišťuje řízení přístupu založené na tom, odkud kód pochází a kdo kód podepsal (řízení přístupu na bázi zdroje kódu). Chcete-li zjistit více informací o používání produktu J2SDK, prohlédněte si téma Java Authentication and Authorization Service for the IBM Developer Kit for Java v aplikaci IBM Systems Software Information Center.

## Zabezpečení aplikací v jazyce Java pomocí SSL

Pomocí protokolu SSL můžete zabezpečit komunikace aplikací systému iSeries, které jste vyvinuli pomocí nástrojů IBM Developer Kit for Java. Výhod protokolu SSL mohou také využívat klientské aplikace, které používají nástroje IBM Toolbox for Java. Proces aktivace SSL u vašich vlastních aplikací v Javě se liší od aktivace u jiných aplikací.

Další informace o administraci protokolu SSL v aplikacích napsaných v jazyce Java najdete v těchto tématech aplikace IBM Systems Software Information Center:

- IBM Toolbox for Java - prostředí SSL (Secure Sockets Layer (SSL).
- IBM Developer Toolkit for Java to make a Java - zabezpečení aplikací pomocí SSL.

**Související pojmy**

“Zabezpečení webových služeb” na stránce 16
Když poskytujete návštěvníkům přístup ke svým webovým stránkám, nechcete jim samozřejmě odhalovat informace o tom, jak jsou vaše stránky nastaveny a jaké kódování je použito k jejich vygenerování.

Digital Certificate Manager

Authentication Services

**Související úlohy**

Zabezpečení aplikací v Javě pomocí SSL

**Související informace**

Java Authentication and Authorization Service

Prostředí SSL (Secure Sockets Layer)

# Zabezpečení elektronické pošty

Použití elektronické pošty v síti Internet nebo v jiné nedůvěryhodné síti představuje bezpečnostní riziko, před kterým vás ochranná bariéra nemusí ochránit.

Těmto rizikům musíte porozumět, abyste si byli jisti, že je vaše strategie zabezpečení ochrany dat bude minimalizovat.

Elektronická pošta se podobá jiným formám komunikace. Je velmi důležité, abyste při zasílání důvěrných informací elektronickou poštou byli uvážliví. Je tomu tak proto, že vaše elektronická pošta prochází mnoha servery, než se k vám dostane, a je možné, aby ji někdo zachytil a přečetl. V důsledku toho budete asi chtít použít bezpečnostní opatření na ochranu důvěrnosti vaší elektronické pošty.

## Běžná rizika zabezpečení elektronické pošty

Některá rizika spojená s použitím elektronické pošty:

- **Záplava** (typ útoku s následkem přerušení síťových služeb) nastává, když je systém přetížen mnoha zprávami elektronické pošty. Pro vetřelce je poměrně snadné vytvořit jednoduchý program, který posílá miliony zpráv elektronické pošty (včetně prázdných zpráv) na jediný poštovní server a pokouší se jej zaplavit. Bez řádného zabezpečení může na cílovém serveru nastat přerušení síťových služeb, protože se disk serveru zaplní zbytečnými zprávami. Anebo může server přestat odpovídat, protože se všechny jeho prostředky zabývají zpracováním pošty v důsledku tohoto napadení.
- **Zasílání nevyžádaných e-mailů (spamming)** je další typ napadení běžný u elektronické pošty. S rostoucím počtem podniků nabízejících elektronický obchod přes Internet jsme byli svědky exploze nežádoucí nebo nevyžádané obchodní elektronické pošty. To je zanášení zásilkami, které se posílají podle rozsáhlého distribučního seznamu uživatelů elektronické pošty a přeplňují jejich schránky.
- **Ochrana důvěrných informací** je vystavena riziku, je-li elektronická pošta zasílána jiné osobě v síti Internet. Taková pošta prochází mnoha servery, než dosáhne zamýšleného příjemce. Pokud jste zprávu nezašifrovali, může ji hacker vyhmátnout a přečíst v kterémkoliv bodu přenosové cesty.

## Volby zabezpečení elektronické pošty

Chcete-li se chránit před rizikem zaplavování a zasílání nevyžádaných e-mailů, musíte patřičně konfigurovat svůj poštovní server. Většina aplikací serveru nabízí metody, jak se s takovým napadením vypořádat. Můžete také spolupracovat se svým poskytovatelem služeb sítě Internet (ISP) a zajistit, aby i on poskytl nějakou další ochranu před těmito útoky.

To, jaká další bezpečnostní opatření potřebujete, závisí na požadované úrovni důvěrnosti a také na tom, jaké zabezpečení poskytují aplikace elektronické pošty. Je například dostačující ponechat obsah zprávy elektronické pošty jako důvěrný? Nebo chcete, aby byly důvěrné všechny informace týkající se elektronické pošty, jako například počáteční a cílové IP adresy?

V některých aplikacích jsou integrovány funkce zabezpečení dat, které mohou zabezpečit potřebnou ochranu. Například produkt Lotus Notes Domino nabízí několik integrovaných funkcí zabezpečení dat včetně schopnosti šifrování celého dokumentu nebo jednotlivých polí v dokumentu.

Při šifrování pošty vytvoří produkt Lotus Notes Domino jedinečný veřejný a soukromý klíč pro každého uživatele. Pomocí soukromého klíče zprávu zašifrujete tak, aby byla čitelná jen pro ty uživatele, kteří mají váš veřejný klíč. Veřejný klíč musíte poslat zamýšleným adresátům vaší zprávy, aby jej mohli použít při jejím dešifrování. Jestliže vám někdo pošle zašifrovanou zprávu, použije produkt Lotus Notes Domino veřejný klíč odesílatele k jejímu dešifrování.

Informace o používání těchto šifrovacích funkcí produktu Notes najdete v online nápovědě k tomuto programu.

Podrobnější informace o zabezpečení produktu Domino na systémech iSeries najdete v těchto referenčních informacích:

- Knihovna referenčních informací Lotus Domino na této adrese URL:
  `http://www.ibm.com/eserver/iseries/domino/library.htm`
- Lotus Notes and Domino R5.0 Security Infrastructure Revealed (SG24-5341)
- Lotus Domino for AS/400 Internet Mail and More (SG24-5990)

Chcete-li pro elektronickou poštu a jiné informace, které kolují mezi pobočkami, vzdálenými klienty nebo obchodními partnery, zajistit vyšší stupeň důvěrnosti, máte několik možností.

Jestliže to aplikace poštovního serveru podporuje, můžete pomocí SSL (Secure Sockets Layer) vytvořit mezi serverem a klienty elektronické pošty zabezpečenou relaci. SSL také poskytuje podporu volitelné autentizace na straně klienta, pokud je aplikace typu klient napsána tak, aby SSL používala. Vzhledem k tomu, že je celá relace zašifrovaná, zajistí SSL integritu i při přenosu dat.

Další možností je nakonfigurovat spojení VPN (Virtual Private Network). Počínaje verzí V4R4 můžete použít server iSeries ke konfiguraci různých spojení VPN, včetně spojení mezi vzdálenými klienty a vaším systémem iSeries. Když používáte VPN, je veškerý provoz plynoucí mezi komunikujícími koncovými body zašifrovaný, což zaručuje důvěrnost a integritu dat.

**Související pojmy**

Virtual private network (VPN)

“Zabezpečení protokolu FTP”
Protokol FTP (File Transfer Protocol) poskytuje schopnost přenosu souborů mezi klientem (uživatelem v jiném systému) a vaším serverem.

“Metoda zabezpečení ochrany dat pomocí vrstvené obrany” na stránce 4
**Strategie zabezpečení ochrany dat** definuje to, co chcete ochránit a to, co očekáváte od uživatelů vašeho systému.

**Související odkazy**

Terminologie zabezpečení

## Zabezpečení protokolu FTP

Protokol FTP (File Transfer Protocol) poskytuje schopnost přenosu souborů mezi klientem (uživatelem v jiném systému) a vaším serverem.

K předání příkazů serveru můžete použít také schopnost předávat vzdálené příkazy. Díky tomu je FTP velmi užitečný při práci se vzdálenými systémy nebo k přesunu souborů mezi systémy. Avšak používání FTP v síti Internet nebo jiných nedůvěryhodných sítích vás vystavuje jistým bezpečnostním rizikům. Těmto rizikům musíte porozumět, abyste si byli jisti, že je vaše strategie zabezpečení ochrany dat bude minimalizovat.

- Když povolíte protokol FTP v systému, může se stát, že vaše schéma oprávnění k objektům nebude poskytovat dostatečnou ochranu.

Například můžete mít u objektů veřejné oprávnění *USE, ale dnes chcete zabránit většině uživatelů v přístupu k nim pomocí funkce ″zabezpečení menu″. (Funkce zabezpečení menu zabraňuje uživatelům dělat něco, co není jednou z voleb jejich menu.) Jelikož uživatelé FTP nejsou odkázáni jen na menu, mohou číst všechny objekty ve vašem systému.

Níže je uvedeno několik voleb pro řízení tohoto bezpečnostního rizika:

- Uplatněte úplné zabezpečení objektů v systému iSeries (jinými slovy, změňte model zabezpečení systému ze ″zabezpečení menu″ na ″zabezpečení objektu″). Je to nejlepší a nejjistější volba.
- Napište programy výstupního bodu pro FTP, kterými omezíte přístup k souborům přenášeným pomocí FTP. Programy výstupních bodů by měly poskytnout aspoň takové zabezpečení, které odpovídá zabezpečení poskytovanému programem menu. Mnoho zákazníků by asi chtělo, aby řízení přístupu FTP bylo ještě restriktivnější. Tato volba se týká pouze FTP, a ne ostatních rozhraní, jako například ODBC, DDM nebo DRDA.

  **Poznámka:** Oprávnění k souboru *USE umožňuje, aby si uživatel soubor mohl stáhnout. Oprávnění k souboru *CHANGE umožňuje, aby uživatel mohl soubor odeslat.

- Hacker může provést útok s následkem ″přerušení síťových služeb″ a přimět váš server FTP, aby zablokoval uživatelské profily v systému. Provádí to tak, že se opakovaně pokouší přihlásit s nesprávným heslem uživatelského profilu, dokud není profil zablokován. Tento typ útoku zablokuje profil, jestliže dosáhne maximálního počtu přihlášení - tří.

  Tohoto rizika se můžete vyvarovat analýzou zvýhodněného zvýšení zabezpečení dat a minimalizace napadení na úkor poskytnutí snadného přístupu uživatelům. Server FTP normálně prosazuje systémovou hodnotu QMAXSIGN, aby hackerům neposkytl neomezený počet pokusů, při nichž by mohli uhodnout heslo a provést pak útok. Níže je uvedeno několik voleb, o jejichž použití byste měli uvažovat:

  - Použijte program výstupního bodu přihlášení k FTP, abyste zamítli požadavky na přihlášení všem uživatelským profilům systému a těm uživatelským profilům, u kterých určíte, že nebudou mít k FTP přístup. (Při použití takového programu výstupního bodu se pokusy o přihlášení zamítnuté programem u zablokovaných uživatelských profilů **nepočítají** v čítači profilu QMAXSIGN.)
  - Použijte program výstupního bodu přihlášení k FTP, abyste omezili počet počítačů klienta, ze kterých má daný uživatelský profil přístup k serveru FTP. Má-li například někdo z účtárny (profil Accounting) přístup k serveru FTP, povolte tomuto uživatelskému profilu přístup k serveru FTP pouze z počítačů, které mají IP adresy v oddělení účtárny.
  - Použijte program výstupního bodu přihlášení k FTP, abyste zapsali do protokolu jméno uživatele a IP adresu u všech pokusů o přihlášení k serveru FTP. Pravidelně tyto protokoly prohlížejte a kdykoliv dojde k zablokování profilu kvůli maximálnímu počtu pokusů s heslem, identifikujte vetřelce na základě informací z IP adresy a učiňte příslušná opatření.
  - Pomocí systému detekujícího vniknutí kontrolujte útoky s následkem ″přerušení síťových služeb″.

Kromě toho můžete výstupní body serveru FTP využít k anonymní funkci FTP pro hostující uživatele. Nastavení zabezpečeného anonymního serveru FTP vyžaduje programy výstupních bodů jak pro přihlášení k serveru FTP, **tak** pro ověření platnosti požadavků na server FTP.

Chcete-li zabezpečit komunikační relace serveru FTP, můžete používat protokol SSL (Secure Sockets Layer). Použití SSL zajistí zašifrování všech přenosů FTP, aby byla zachována důvěrnost všech dat, která procházejí mezi serverem FTP a klientem, včetně jména uživatele a hesla. Server FTP také podporuje použití digitálních certifikátů včetně autentizace klienta.

Kromě těchto voleb FTP můžete zvážit použití anonymního FTP, které uživatelům zajistí pohodlný a jednoduchý způsob přístupu k materiálům, které nejsou důvěrné. Anonymní FTP povolí nechráněný přístup (není vyžadováno heslo) k vybraným informacím ve vzdáleném systému. Vzdálený server určí, jaké informace budou všeobecně dostupné. Tyto informace jsou považovány za veřejně přístupné a mohou být čteny kýmkoliv. Předtím, než budete konfigurovat anonymní server FTP, byste měli odhadnout bezpečnostní rizika a zvážit možnost zabezpečení serveru FTP pomocí programů výstupního bodu.

- Konfigurace anonymního FTP.
- Správa přístupu pomocí FTP programů výstupního bodu.

Chcete-li se dozvědět více o použití FTP, rizicích a dostupných bezpečnostních opatřeních, prostudujte si tato témata:

- Téma Implementace zabezpečení FTP v rámci aplikace IBM Systems Software Information Center.
- Téma Anonymní FTP v rámci aplikace IBM Systems Software Information Center.
- Téma Zabezpečení FTP pomocí SSL v rámci aplikace IBM Systems Software Information Center.

**Související pojmy**

“Zabezpečení elektronické pošty” na stránce 20
Použití elektronické pošty v síti Internet nebo v jiné nedůvěryhodné síti představuje bezpečnostní riziko, před kterým vás ochranná bariéra nemusí ochránit.

Virtual private network (VPN)

“Metoda zabezpečení ochrany dat pomocí vrstvené obrany” na stránce 4
**Strategie zabezpečení ochrany dat** definuje to, co chcete ochránit a to, co očekáváte od uživatelů vašeho systému.

Detekování vniknutí

**Související odkazy**

Terminologie zabezpečení

## Volby zabezpečení přenosu dat

Obsahuje informace o bezpečnostních opatřeních, která můžete aplikovat při ochraně dat, když procházejí přes nedůvěryhodné sítě, jako je například Internet. K těmto opatřením patří připojení pomocí protokolu SSL (Secure Sockets Layer), produkt iSeries Access Express a připojení VPN (Virtual Private Network).

Připomeňte si, že ve scénáři má firma JKL Toy dva primární systémy iSeries. Jeden používá pro vývoj a druhý pro výrobní aplikace. Oba systémy pracují s životně důležitými daty a aplikacemi. Proto bylo přijato rozhodnutí přidat do okrajové sítě nový systém iSeries obsluhující intranetové a internetové aplikace.

Vytvoření okrajové sítě zajistí určité fyzické oddělení interní sítě firmy od sítě Internet. Takové oddělení snižuje riziko plynoucí z používání Internetu, vůči kterému jsou interní systémy zranitelné. Vymezením nového serveru iSeries jako výlučně internetového serveru snižuje firma také složitost správy zabezpečení své sítě.

Vzhledem k naléhavé potřebě ochrany dat v prostředí sítě Internet pracuje společnost IBM průběžně na vývoji nabídky produktů, které by zajistily zabezpečení prostředí v sítích provozujících elektronické podnikání v síti Internet. V prostředí sítě Internet musíte zabezpečit ochranu jak systému, tak aplikací. Pohyb důvěrných informací ve vnitropodnikové síti nebo přes internetové spojení však dále zvyšuje potřebu implementace účinnějších bezpečnostních řešení. Chcete-li tato rizika potlačit, měli byste implementovat bezpečnostní opatření na ochranu přenosu dat, která procházejí sítí Internet.

Rizika spojená s pohybem informací po nedůvěryhodných systémech můžete minimalizovat pomocí dvou specifických položek nabídky zabezpečení systému iSeriesna úrovni přenosu: zabezpečení komunikací pomocí protokolu SSL (Secure Sockets Layer) a připojení VPN (Virtual Private Networking).

### Zabezpečení aplikací pomocí SSL

Protokol SSL (Secure Sockets Layer) je de facto odvětvová norma pro zabezpečení komunikace mezi klienty a servery. Protokol SSL byl původně vyvinut pro aplikace prohlížeče WWW, ale v současné době jej může používat stále rostoucí počet aplikací. Na serveru iSeries mezi ně patří:

- Server IBM HTTP Server for iSeries (původní a provozovaný na bázi Apache).
- Server FTP.
- Server Telnet.
- DRDA (distributed relational database architecture) (DRDA) a DDM (distributed data management).
- Server (DDM).
- Centrální správa v prostředí produktu iSeries Navigator.
- LDAP (Directory Services Server).

- Aplikace produktu iSeries Access Express, včetně iSeries Navigator, a aplikace, které byly napsány do sady rozhraní API iSeries Access Express.
- Programy vyvinuté pomocí nástroje Developer Kit for Java a klientské aplikace, které používají IBM Toolkit for Java.
- Programy vyvinuté pomocí rozhraní API SSL (Secure Sockets Layer), které je možné použít k aktivaci SSL u aplikací. Další informace o tom, jak psát programy používající protokol SSL, najdete v tématu Rozhraní API protokolu SSL (Secure Sockets Layer).

Několik těchto aplikací také podporuje používání digitálních certifikátů pro autentizaci klienta. Protokol SSL spoléhá při autentizaci účastníků komunikace a při vytváření zabezpečeného spojení na digitální certifikáty.

**VPN (Virtual Private Networking) v systému iSeries**

Systém iSeries můžete použít k připojení VPN, chcete-li vytvořit zabezpečený komunikační kanál mezi dvěma koncovými body. Podobně jako u spojení SSL mohou být data, která putují mezi dvěma koncovými body, zašifrovaná, což zaručuje jejich důvěrnost a integritu. Spojení VPN vám však umožňují omezit postup provozu ke koncovým bodům, které specifikujete, a omezit typ provozu, který může spojení použít. Proto poskytuje spojení VPN jisté zabezpečení na úrovni sítě tím, že vám pomáhá chránit síťové prostředky před neoprávněným přístupem.

**Jakou metodu byste měli použít?**

Obě tyto metody zabezpečení se zabývají potřebami zajištění autentizace, důvěrnosti a integrity dat. To, kterou z těchto metod byste měli použít, závisí na několika faktorech. Mezi faktory, které je nutno vzít v úvahu, patří to, s kým komunikujete, jaké aplikace pro tuto komunikaci používáte, jak zabezpečené musí komunikace být a jaká zvýhodnění na úkor nákladů a výkonu jste ochotni udělat, aby tato komunikace byla zajištěna.

Rovněž, chcete-li použít specifickou aplikaci se SSL, musí být tato aplikace na použití SSL nastavena. Ačkoliv mnohé aplikace ještě nemohou využívat výhod protokolu SSL, mnoho jiných, jako např. Telnet a iSeries Access Express, tuto přidanou schopnost využívání protokolu SSL mají. Na druhé straně vám VPN umožňuje chránit veškerý provoz IP, který postupuje mezi koncovými body specifického spojení.

Můžete například použít HTTP přes SSL a umožnit tak běžně obchodnímu partnerovi komunikovat s webovým serverem ve vaší interní síti. Jestliže je webový server jedinou zabezpečenou aplikací, kterou potřebujete pro komunikaci se svým obchodním partnerem, pak asi nebudete potřebovat přejít na spojení VPN. Pokud byste však chtěli své komunikace rozšířit, budete muset spojení VPN přece jen použít. Může také nastat situace, kdy budete potřebovat ochránit provoz v části své sítě, ale nebudete chtít konfigurovat individuálně každého klienta a každý server, aby používaly SSL. Pro tuto část sítě byste také mohli vytvořit VPN spojení od jedné přenosové brány k druhé. To by zabezpečilo provoz, ale spojení zůstává transparentní pro individuální servery a klienty na obou stranách.

**Související pojmy**

“Metoda zabezpečení ochrany dat pomocí vrstvené obrany” na stránce 4
**Strategie zabezpečení ochrany dat** definuje to, co chcete ochránit a to, co očekáváte od uživatelů vašeho systému.

“Scénář: Plán elektronického podnikání firmy JKL Toy Company” na stránce 8
Popisuje typickou firmu se jménem JKL Toy, která se rozhodla rozšířit své obchodní záměry používáním sítě Internet. I když jde o fiktivní společnost, jsou její plány na využití sítě Internet pro elektronické podnikání a z toho vyplývající potřeby zabezpečení ochrany dat reprezentativní pro situaci mnoha firem v reálném světě.

“Použití digitálních certifikátů pro SSL” na stránce 25
Digitální certifikáty jsou základem pro používání vrstvy SSL (Secure Sockets Layer) pro bezpečnou komunikaci a jsou také silným nástrojem autentizace.

“Zabezpečení soukromých komunikací pomocí VPN” na stránce 26
Chcete-li v rámci své organizace důvěrně a bezpečně komunikovat, můžete použít sítě VPN (Virtual Private Network).

**Související odkazy**

Rozhraní API protokolu SSL (Secure Sockets Layer)

# Použití digitálních certifikátů pro SSL

Digitální certifikáty jsou základem pro používání vrstvy SSL (Secure Sockets Layer) pro bezpečnou komunikaci a jsou také silným nástrojem autentizace.

Server iSeries nabízí možnost snadno vytvářet a spravovat digitální certifikáty pro vaše systémy a uživatele pomocí aplikace Digital Certificate Manager (DCM), integrované funkce systému i5/OS.

Dále můžete nakonfigurovat některé aplikace, jako například IBM HTTP Server for iSeries,tak, aby používaly digitální certifikáty jako účinnější metodu autentizace klienta namísto jména uživatele a jeho hesla.

## Co je to digitální certifikát?

Digitální certifikát je digitální ověření, které potvrzuje identitu vlastníka certifikátu, podobně jako cestovní pas. Důvěryhodný třetí účastník, nazývaný jako **vydavatel certifikátů (CA),** vydává digitální certifikáty uživatelům a serverům. Důvěra ve vydavatele (CA) je základem důvěry v certifikát jako platné pověření.

Každý CA má svou strategii, jak určit, jaké identifikační informace bude požadovat, aby certifikát vydal. Někteří CA v síti Internet mohou požadovat velmi málo informací, např. požadují jen rozlišovací jméno. Je to jméno osoby nebo serveru, kterému vydavatel certifikátu vydá adresu digitálního certifikátu a digitální adresu elektronické pošty. Pro každý certifikát se generuje soukromý a veřejný klíč. Certifikát obsahuje veřejný klíč, zatímco prohlížeč nebo zabezpečený soubor ukládá soukromý klíč. Tyto páry klíčů, které jsou přidruženy k příslušnému certifikátu, lze používat k ″podpisu″ a zašifrování dat, jako jsou například zprávy a dokumenty posílané mezi uživateli a servery. Digitální podpisy zajišťují spolehlivost původu položky a chrání její integritu.

Další informace o používání produktu Digital Certificate Manager najdete v aplikaci IBM Systems Software Information Center.

Ačkoliv mnohé aplikace ještě nemohou využívat výhod protokolu SSL, mnoho jiných, jako např. Telnet a iSeries Access Express, tuto přidanou schopnost využívání protokolu SSL mají. Chcete-li zjistit, jak používat protokol SSL v aplikacích iSeries, prostudujte si téma **Zabezpečení aplikací pomocí SSL** v rámci aplikace IBM Systems Software Information Center.

**Související pojmy**

“Volby zabezpečení přenosu dat” na stránce 23

Obsahuje informace o bezpečnostních opatřeních, která můžete aplikovat při ochraně dat, když procházejí přes nedůvěryhodné sítě, jako je například Internet. K těmto opatřením patří připojení pomocí protokolu SSL (Secure Sockets Layer), produkt iSeries Access Express a připojení VPN (Virtual Private Network).

Digital Certificate Manager

Zabezpečení aplikací pomocí SSL

**Související odkazy**

Terminologie zabezpečení

## Zabezpečený přístup k Telnetu pomocí SSL

Chcete-li zabezpečit komunikační relace Telnet, můžete nakonfigurovat server Telnet tak, aby používal protokol SSL (Secure Sockets Layer).

Chcete-li nakonfigurovat server Telnet, aby používal SSL, musíte použít produkt DCM (Digital Certificate Manager) a nakonfigurovat certifikát, který bude server Telnet používat. Server Telnet obsluhuje standardně jak zabezpečená, tak nezabezpečená připojení. Server Telnet však můžete konfigurovat tak, aby povoloval jen zabezpečené relace Telnet. Kromě toho můžete server konfigurovat tak, aby kvůli lepší autentizaci klientů používal digitální certifikáty.

Když zvolíte použití SSL u serveru Telnet, dosáhnete výrazného přínosu pro zabezpečení ochrany dat. U serveru Telnet se navíc k autentizaci serveru šifrují data předtím, než dojde k řízení toku dat protokolem Telnet. Jakmile se relace SSL zavede, zašifrují se všechny protokoly Telnet, včetně výměny ID uživatele a hesla.

Nejdůležitějším faktorem k uvážení při použití serveru Telnet je citlivost informací, které budete používat během relace klienta. Jde-li o citlivé nebo soukromé informace, může být pro vás výhodné nastavit server iSeries Telnet tak, aby používal SSL. Když pro aplikaci Telnet nakonfigurujete digitální certifikát, je server Telnet schopen obsluhovat jak klienty, kteří mají protokol SSL, tak i klienty, kteří protokol SSL nemají. Jestliže vaše strategie zabezpečení ochrany dat vyžaduje, abyste relace Telnet vždy šifrovali, můžete všechny relace Telnet bez SSL zašifrovat. Když nebude potřeba, abyste server SSL Telnet používali, můžete port SSL vypnout. Porty je možné uzavřít příkazem ADDTCPPORT. Jakmile port vypnete, poskytuje server klientům Telnet bez SSL a relace SSL Telnet jsou zablokované.

Téma Telnet v aplikaci IBM Systems Software Information Center poskytuje informace, které potřebujete při používání serveru Telnet na serveru iSeries.

**Související pojmy**

Zabezpečení Telnetu

Digitální certifikát

### SSL pro zabezpečení produktu iSeries Access Express

Servery iSeries Access Express můžete nakonfigurovat tak, aby používaly protokol SSL (Secure Sockets Layer) k zabezpečení komunikačních relací iSeries Access Express.

Použití SSL zajistí, aby byl veškerý provoz relací iSeries Access Express zašifrovaný. To znemožňuje přečíst data procházející mezi lokálními a vzdálenými uzly.

Další informace o použití produktu iSeries Access Express s protokolem SSL najdete v těchto tématech aplikace IBM Systems Software Information Center :

- Administrace SSL (Secure Sockets Layer)
- IBM Developer Kit for Java SSL
- IBM Java Toolbox SSL

## Zabezpečení soukromých komunikací pomocí VPN

Chcete-li v rámci své organizace důvěrně a bezpečně komunikovat, můžete použít sítě VPN (Virtual Private Network).

Protože firma JKL Toy stále větší měrou používá VPN a zabezpečení ochrany dat, které VPN nabízí, hledá nyní možnost přenosu dat prostřednictvím sítě Internet. Nedávno koupila další malou firmu na výrobu hraček a chce ji provozovat jako svou pobočku. Firma JKL Toy bude potřebovat předávat si s pobočkou informace. Obě firmy používají servery iSeries a použití spojení VPN může zajistit zabezpečení dat potřebné pro komunikaci mezi oběma sítěmi. Vytvoření VPN je z hlediska nákladů výhodnější než tradiční pronajaté linky.

Spojením VPN můžete řídit a zabezpečit spojení s kancelářemi pobočky, mobilními zaměstnanci, dodavateli, obchodními partnery a dalšími osobami.

Jmenujme některé uživatele, kteří by měli prospěch z použití VPN pro připojitelnost:

- Vzdálení a mobilní uživatelé.
- Domácí kancelář komunikující s kancelářemi pobočky nebo jinými externími pracovišti.
- Komunikace mezi podniky.

Jestliže neomezíte přístup uživatelů k citlivým systémům, vyskytnou se bezpečnostní rizika. Jestliže nevymezíte, kdo může mít k systému přístup, zvyšujete pravděpodobnost toho, že důvěrnost vašich informací nebude zachována. Potřebujete plán, který povolí přístup k systému pouze těm, kdo informace v tomto systému sdílejí. VPN vám umožňuje řídit síťový provoz a přitom nabízí důležité funkce zabezpečení dat, jako například autentizaci a soukromí dat. Vytvoření několika spojení VPN vám umožňuje řídit, kdo v nich bude mít přístup k jednotlivým systémům. Například, účtárna a osobní oddělení mohou být spojeny vlastní sítí VPN.

Když uživatelům povolíte, aby se k systému připojili přes Internet, může dojít k tomu, že budete veřejnými sítěmi posílat citlivá data společnosti, která tak mohou být napadena. Jednou z voleb, jak ochránit přenášená data, je použít metody šifrování a autentizace k zajištění soukromí a zabezpečení před vnějšími zásahy. Spojení VPN nabízí řešení specifické potřeby ochrany dat - zabezpečení komunikace mezi systémy. Spojení VPN poskytuje ochranu pro data, která postupují mezi dvěma koncovými body spojení. Mimoto můžete použít zabezpečení pomocí pravidel paketů a definovat, které IP pakety smějí sítí VPN procházet.

VPN můžete použít, chcete-li vytvořit zabezpečené spojení mezi řízenými a důvěryhodnými koncovými body. Přesto musíte neustále zvažovat, kolik možností přístupu svým partnerům ve VPN poskytnete. spojení VPN může zakódovat data, která procházejí veřejnými sítěmi. Ale podle toho, jak je nakonfigurujete, nemusí být data přicházející z Internetu, přenášena přes připojení VPN. V takovém případě by tato data neměla být šifrována, protože prochází přes interní sítě, jež komunikují prostřednictvím těchto připojení. V důsledku toho byste měli pečlivě naplánovat, jak jednotlivá spojení VPN nastavit. Dbejte na to, abyste svému partnerovi ve VPN poskytli přístup jenom k těm hostitelům nebo prostředkům vaší interní sítě, u kterých si to přejete.

Můžete mít například prodejce, který potřebuje získat informace o tom, jaké díly máte na skladě. Tyto informace máte v databázi, kterou používáte k aktualizaci webových stránek ve vaší vnitropodnikové síti. Chtěli byste prodejci povolit přístup k těmto stránkám přímo přes spojení VPN. Nechcete však, aby měl přístup k jiným systémovým prostředkům, jako například k samotné databázi. Naštěstí můžete spojení VPN konfigurovat tak, že provoz mezi oběma koncovými body je omezen na port 80. Port 80 je standardní port, který používá provoz HTTP. V důsledku toho může váš prodejce odesílat a přijímat požadavky HTTP pouze přes toto spojení.

Díky tomu, že můžete omezit typ provozu, který prochází spojením VPN, zabezpečuje toto spojení ochranu na úrovni sítě. VPN však nepracuje stejným způsobem jako ochranná bariéra při regulaci provozu do systému a ze systému. Připojení VPN není jediným dostupným prostředkem pro zabezpečení komunikace mezi vaším serverem iSeries a jinými systémy. Podle potřeb vašeho zabezpečení ochrany dat můžete dojít k závěru, že vám lépe vyhovuje použití SSL.

To, zda spojení VPN poskytuje zabezpečení, které potřebujete, záleží na tom, co chcete ochránit. Závisí to také na změnách, které jste ochotni udělat, abyste požadovaného zabezpečení dosáhli. Tak, jako u všech rozhodnutí, která se týkají zabezpečení ochrany dat, byste měli zvážit, jak spojení VPN podporuje strategii zabezpečení ochrany vašich dat.

Chcete-li se dozvědět více o připojeních VPN, prostudujte si téma *VPN (Virtual Private Networking)* v aplikaci IBM Systems Software Information Center.

**Související pojmy**

"Volby zabezpečení přenosu dat" na stránce 23

Obsahuje informace o bezpečnostních opatřeních, která můžete aplikovat při ochraně dat, když procházejí přes nedůvěryhodné sítě, jako je například Internet. K těmto opatřením patří připojení pomocí protokolu SSL (Secure Sockets Layer), produkt iSeries Access Express a připojení VPN (Virtual Private Network).

Virtual private networks (VPN)

## Terminologie zabezpečení

Toto téma obsahuje termíny a definice související s informacemi týkajícími se zabezpečení ochrany dat.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

**A**

**authentication (autentizace)**
Ověření, že vzdálený klient nebo server je skutečně tím, za koho se vydává. Autentizace zajistí, že můžete důvěřovat vzdálenému serveru peer, ke kterému se připojujete.

**B**

**C**

**certificate authority (CA, vydavatel certifikátů)**
Důvěryhodný úřad, který vydává a spravuje bezpečnostní pověření nazývaná digitální certifikáty.

**cipher (šifra)**
Jiný termín pro šifrovací algoritmus.

**ciphertext (šifrovaný text)**
Zašifrovaný text nebo data.

**cracker**
Počítačový fanda, který má špatné úmysly.

**cryptography (šifrování)**
Věda zabývající se zabezpečením dat. Šifrování umožňuje ukládat informace nebo komunikovat s jinými účastníky a zajistit, aby účastníci, kterých se to netýká, uloženým informacím ani vaší komunikaci neporozuměli. Šifrování transformuje srozumitelný text do nesrozumitelných dat (zašifrovaný text). Dešifrování rekonstruuje z nesrozumitelných dat srozumitelný text. Oba procesy zahrnují matematický vzorec nebo algoritmus a tajnou posloupnost dat (klíč).

Existují dva typy šifrování:

- **Symetrické**: Komunikující strany sdílí tajný klíč, který obě používají jak pro šifrování, tak i pro dešifrování. Nazývá se také šifrování pomocí sdíleného klíče.
- **Asymetrické**: Každý člen komunikující skupiny má dva klíče: veřejný klíč a soukromý klíč. Mezi oběma klíči je matematická souvislost, ale je prakticky nemožné soukromý klíč z veřejného klíče odvodit. Zprávu, která je zašifrovaná něčím veřejným klíčem, je možné dešifrovat pouze přidruženým soukromým klíčem. Alternativně může server nebo uživatel použít soukromý klíč k ″podpisu″ dokumentu a pomocí veřejného klíče digitální podpis dešifrovat. Pokud přepočet klíče, který je výsledkem dešifrování podpisu pomocí veřejného klíče, odpovídá reálné hodnotě přepočtu klíče vlastního dokumentu, je podpis považován za platný a zdroj dokumentu se považuje za ověřený. Nazývá se také šifrování pomocí veřejného klíče.

**D**

**data confidentiality (utajení dat)**
Ukrývá obsah zprávy, obvykle pomocí šifrování.

**data integrity (integrita dat)**
Ověřuje, že obsah datagramu nebyl během přenosu změněn, ať už záměrně, nebo díky náhodným chybám.

**data origin authentication (autentizace původu dat)**
Ověřuje, že IP datagram pochází od proklamovaného odesílatele.

**denial of service attack (napadení s následkem přerušení síťových služeb)**
Nazývá se také napadení DoS. Způsobí, že služba, jako např. webový server, bude přerušena nebo nepoužitelná, protože síť bude zahlcena zbytečným provozem IP.

**digital certificate (digitální certifikát)**
Digitální dokument, který ověřuje totožnost vlastníka certifikátu, podobně jako cestovní pas. Důvěryhodný účastník zvaný vydavatel certifikátu (CA) vydává digitální certifikáty uživatelům a serverům. Důvěra ve vydavatele (CA) je základem důvěry v certifikát jako platné pověření. Můžete je použít k následujícím účelům:

- Identifikace - kdo je uživatel.
- Autentizace - jistota, že uživatel je tím, za koho se prohlašuje.
- Integrita - určení, zda byl obsah dokumentu změněn, ověřením digitálního podpisu odesílatele.
- Neodmítání - záruka, že uživatel nemůže tvrdit, ze neprovedl nějakou akci. Uživatel nemůže například popřít, že poskytl oprávnění k elektronickému nákupu pomocí kreditní karty.

**digital signature (digitální podpis)**
Rovnocenný s osobním podpisem na písemném dokumentu. Digitální podpis poskytuje důkaz o původu

dokumentu. Vlastník certifikátu ″podepíše″ dokument tak, že použije soukromý klíč přidružený k certifikátu. Příjemce dokumentu použije odpovídající veřejný klíč, aby podpis dešifroval, čímž ověří odesilatele jakožto zdroj.

**Digital Certificate Manager (DCM)**
Tento produkt umožňuje, aby systém iSeries vystupoval jako lokální vydavatel certifikátů (CA). Pomocí DCM můžete vytvořit digitální certifikáty pro servery nebo uživatele. Můžete importovat digitální certifikáty, které vydali jiní CA. Digitální certifikát můžete připojit také k uživatelskému profilu systému i5/OS. Pomocí DCM můžete také konfigurovat aplikace tak, aby pro zabezpečení komunikace používaly SSL (Secure Sockets Layer).

**distinguished name (rozlišovací jméno)**
Jméno osoby nebo serveru, kterému vydavatel certifikátů vydal digitální certifikát. Certifikát poskytuje toto jméno pro označení vlastnictví certifikátu. Podle strategie CA, který certifikát vydává, může rozlišovací jméno zahrnout i další informace o oprávnění.

**Domain Name System (DNS)**
Sada dat, která se používá k identifikaci jednotlivých držitelů digitálních certifikátů. V rámci digitálních certifikátů třídy 1 obsahuje informace, jako jméno a elektronická adresa, a vydavatele digitálního certifikátu (VeriSign, Inc.).

Když se připojíte k Internetu, použije váš internetová klient server DNS, aby určil IP adresu hostitelského systému, se kterým chcete komunikovat.

**E**

**encryption (šifrování)**
Proces transformace dat do tvaru, který je nečitelný pro každého, kdo nevlastní správnou metodu a klíč pro dešifrování. Neoprávnění účastníci mohou přesto informace zachytit. Avšak bez správné metody a klíče pro dešifrování jsou informace nesrozumitelné.

**Enterprise Identity Mapping (EIM)**
EIM je mechanismus mapování (přidružování) osoby nebo entity na odpovídající totožnosti uživatelů v různých registrech uživatelů v celém podniku. EIM obsahuje rozhraní API pro vytváření a správu těchto vztahů mapování totožnosti, a rozhraní API, která používají aplikace k získání těchto informací.

**extranet**
Soukromá podniková síť několika spolupracujících organizací, umístěná mimo společnou ochrannou bariéru. Služba extranet používá stávající infrastrukturu Internetu, včetně standardních serverů, klientů elektronické pošty a prohlížečů WWW. Díky tomu je extranet úspornější než vytvoření a údržba soukromé sítě. Dovoluje obchodním partnerům, dodavatelům a zákazníkům se společným zájmem používat rozšířený Internet a vytvářet jednak těsné obchodní vztahy, jednak silný komunikační svazek.

**F**

**firewall (ochranná bariéra)**
Logická bariéra mezi vaší interní sítí a externí sítí, jako například Internetem. Ochrannou bariéru tvoří jeden nebo více hardwarových a softwarových systémů nebo logických částí. Ovládá přístup a tok informací mezi zabezpečenými nebo důvěryhodnými systémy a nezabezpečenými a nedůvěryhodnými systémy.

**G**

**H**

**hacker** Každá osoba, která se neoprávněně pokouší proniknout do vašeho systému.

**hypertext links (hypertextové odkazy)**
Způsob online nabídky informací pomocí propojení (zvaných hypertextové odkazy) mezi jednou informací (zvanou hypertextový uzel) a jinou informací.

**Hypertext Markup Language (HTML)**
Jazyk, který se používá při definování hypertextových dokumentů. Pomocí jazyka HTML můžete označit, jak by váš dokument měl vypadat (například zvýraznění a druh písma) a jak by měl být spojen s jinými dokumenty nebo objekty.

**Hypertext Transfer Protocol (HTTP)**
Standardní metoda přístupu k hypertextovým dokumentům.

**I**

**Internet**
Celosvětová ″síť sítí″, které jsou navzájem spojeny. A rovněž sada spolupracujících aplikací, které počítačům připojeným k této ″síti sítí″ umožňují vzájemně komunikovat. Internet nabízí informace k prohlížení, přenos souborů, vzdálené přihlášení, elektronickou poštu, zprávy a další služby. Internetu se často říká jen ″Net″.

**Internet client (internetový klient)**
Program (nebo uživatel), který používá Internet, zadává požadavky programu na serveru Internetu a přijímá od něj výsledky. Jsou k dispozici různé programy klienta, od nichž je možné vyžadovat různé typy internetových služeb. Jedním typem klientského programu je prohlížeč WWW. Jiným je protokol pro přenos souborů (FTP).

**Internet host (internetový hostitelský systém)**
Počítač, který je připojen k síti Internet nebo intranet. Internetový hostitelský systém může provádět více než jeden program internetového serveru. Internetový hostitelský systém může například provozovat server FTP a odpovídat na požadavky aplikací typu klient FTP. Stejný hostitelský systém by mohl provozovat server HTTP a odpovídat na požadavky od klientů používajících prohlížeče WWW. Programy serverů se v hostitelském systému typicky spouštějí na pozadí (v dávkách).

**Internet Key Exchange (IKE) protocol (protokol IKE)**
Podporuje automatické vyjednávání zabezpečovacích asociací, stejně jako automatické generování a aktualizaci šifrovacích klíčů v rámci VPN (virtual private networking).

**Internet name (internetové jméno)**
Alias pro IP adresu. IP adresa je dlouhý numerický útvar a je obtížné si ji zapamatovat, jako například 10.5.100.75. Tuto IP adresu můžete přiřadit internetovému jménu, jako například system1.vnet.ibm.com. Internetové jméno se také nazývá plně kvalifikované jméno domény. Když uvidíte reklamu, která říká ″Navštivte naši domovskou stránku″, pak adresa domovské stránky obsahuje internetové jméno, nikoli IP adresu, protože internetové jméno se snáze zapamatuje. Plně kvalifikované jméno domény má několik částí. Například system1.vnet.ibm.com má tyto části:

**com:** Všechny komerční sítě. Tuto část jména domény přiřazuje externí organizace, které se říká IA (Internet authority). Různým druhům sítí se přiřazují různé znaky (jako například *com* komerčním a *edu* vzdělávacím institucím).

**ibm:** Identifikátor organizace. Tuto část jména domény také přiřazuje IA (Internet authority) a je jedinečná. Jen jedna organizace na světě může mít identifikátor ibm.com.

**vnet:** Seskupení systémů uvnitř ibm.com. Tento identifikátor se přiřadí interně. Správce ibm.com může vytvořit jedno nebo více seskupení.

**system1:**
Jméno internetového hostitelského systému uvnitř skupiny vnet.ibm.com.

**Internet server (internetový server)**
Program (nebo sada programů), který přijímá požadavky od odpovídajících klientských programů přes Internet a přes Internet těmto klientům odpovídá. Internetový server si můžete představit jako počítač, ke kterému může mít internetový klient přístup nebo jej může navštívit. Různé programy serveru podporují různé služby, jako například:

- Prohlížení (″domovské stránky″ a odkazů na jiné dokumenty a objekty).
- Přenos souborů. Klient může například požadovat přenos souborů ze serveru na klienta. Soubory mohou být softwarové aktualizace, výpisy nebo dokumenty.
- Elektronický obchod, jako například možnost požádat o informace nebo objednat produkty.

**Internet service provider (ISP, poskytovatel služeb sítě Internet)**
Organizace, která poskytuje připojení k síti Internet podobně, jako vaše místní telefonní společnost poskytuje připojení k celosvětové telefonní síti.

**intranet**
Vnitropodniková interní síť, která používá internetové nástroje, jako například prohlížeč WWW nebo protokol FTP.

**intrusion detection (detekování vniknutí)**
Široký termín zahrnující detekci mnoha nežádoucích aktivit. Cílem vniknutí by mohlo být získání informací, ke kterým nemá příslušná osoba oprávnění přístupu (ukradení informací). Cílem by mohlo být způsobení obchodní újmy tím, že síť, systém nebo aplikace bude nedostupná (přerušení služeb), nebo by mohlo jít o získání neoprávněného použití systému jako prostředku k dalšímu vniknutí někam jinam. Většina vniknutí používá tento vzorec: shromažďování informací, pokusy o přístup a destruktivní útoky. Některé útoky může cílový systém detekovat a neutralizovat. Jiné útoky cílový systém nemůže efektivně detekovat a neutralizovat. Většina útoků také používá ″lákací″ pakety, které nelze snadno vystopovat až k jejich skutečnému původci. Řada útoků nyní používá bezděčné spolupachatele, což jsou počítače nebo sítě, které vetřelci používají bez autorizace, aby skryli svou totožnost. Z těchto důvodů je detekování shromažďování informací, pokusů o přístup a chování podobnému útokům životně důležitou částí detekce vniknutí.

**IP address (IP adresa)**
Jedinečný identifikátor sítě TCP/IP (Internet je obrovská síť TCP/IP). Internetový server má obvykle přiřazenou jedinečnou IP adresu. Internetový klient by mohl používat dočasnou, ale jedinečnou IP adresu, kterou přiděluje poskytovatel služeb sítě Internet (ISP).

**IP datagram**
Informační jednotka, která je odeslána po síti TCP/IP. IP datagram (také nazývaný paket) obsahuje jak data, tak informace záhlaví, jako například IP adresy původu a místa určení.

**IP filters (filtry IP)**
Řídí, který IP provoz může vstupovat a vystupovat do a z vaší sítě tak, že filtrují pakety podle pravidel, které jste nadefinovali. Tím chrání zabezpečenou síť před cizími jedinci, kteří používají nekomplikované techniky (např. snímání zabezpečených serverů), nebo i nejsložitější techniky (jako například vylákání IP adresy). O funkci filtrování byste měli uvažovat jako o základu, na kterém se konstruují ostatní nástroje. Poskytuje infrastrukturu, ve které fungují, a odepře přístup všem, snad s výjimkou nejvíce cílevědomého hackera.

**IP security (IPSec) protocol (protokol IPSec)**
Sada protokolů na podporu zabezpečení výměny paketů v síťové vrstvě. IPSec je sada standardů, které používá systém i5/OS a řada dalších systémů k provádění VPN.

**IP spoofing (vylákání IP)**
Pokus o přístup do vašeho systému předstíráním, že jde o systém (IP adresu), které normálně důvěřujete. Potenciální vetřelec nastaví systém s IP adresou, které důvěřujete. Výrobci směrovačů vypracovali a vestavěli do svých systémů ochranu k detekování a odmítnutí pokusů o vylákání.

**J**

**K**

**L**

**M**

**N**

**network address translation (NAT, převod síťových adres)**
Poskytuje transparentnější alternativu k serverům proxy a SOCKS. Zjednodušuje také konfiguraci sítě tím, že povoluje připojení sítí s nekompatibilním členěním adresování. NAT nabízí dvě hlavní funkce. NAT vám tuto ochranu poskytne tím, že vám umožní skrýt ″pravou″ adresu vašeho serveru za adresu, kterou dáváte k dispozici veřejnosti. Může například ochránit veřejný webový server, který chcete provozovat zevnitř vaší interní sítě. NAT také poskytuje mechanismus, aby interní uživatelé měli přístup k Internetu a přitom skryli

soukromé interní IP adresy. NAT poskytuje ochranu, když povolíte interním uživatelům přístup k internetovým službám, protože můžete skrýt jejich soukromé adresy.

**non-repudiation (neodmítání)**
Poskytuje důkaz toho, že transakce proběhla, nebo že jste odeslali nebo přijali zprávu. Použití digitálních certifikátů a kryptografie s veřejným klíčem k ″podpisu″ transakcí, zpráv a dokumentů neodmítání podporuje.

**O**

**P**

**paket** Informační jednotka, která je odeslána po síti TCP/IP. Paket (také nazývaný datagram) obsahuje jak data, tak i informace záhlaví, jako například IP adresy původu a místa určení, a obsahuje také informace o protokolu linky, jako např. Ethernet, token-ring, nebo přenos rámce.

**proxy server**
TCP/IP aplikace, která opakovaně posílá požadavky a odpovědi mezi klienty v zabezpečené interní síti a servery v nedůvěryhodné síti. Proxy server přeruší spojení TCP/IP, aby skryl informace o vaší interní síti (jako například interní IP adresy). Hostitelské systémy mimo vaši síť vnímají proxy server jako zdroj komunikace.

**public key infrastructure (PKI, infrastruktura veřejného klíče)**
Systém digitálních certifikátů, CAs a dalších registračních institucí, které ověřují a prokazují pravost a platnost každého účastníka v internetové transakci.

**Q**

**R**

**replay protection (ochrana před přehráním)**
Zajišťuje, že vetřelec nebude moci zachytit datagram a přehrát ho později.

**S**

**SSL (Secure Sockets Layer)**
Protokol SSL, vytvořený společností Netscape, je de facto odvětvovou normou pro kódování relace mezi klienty a servery. SSL používá k zašifrování relace mezi serverem a klientem (uživatelem) kódování podle metrického klíče. Klient a server vyjednávají o tomto klíči během výměny digitálních certifikátů. Pro každou relaci SSL klienta a serveru se vytvoří odlišný klíč. V důsledku toho, i kdyby neoprávnění uživatelé klíč relace zachytili a dešifrovali (což není pravděpodobné), nemohou jej použít k odposlouchávání současných, budoucích, ani minulých relací SSL.

**single sign-on (SSO, jednotné přihlášení)**
Forma autentizace, která dovoluje uživateli se autentizovat jednou a získat přístup ke zdrojům a prostředkům na více systémech nebo aplikacích. Viz Enterprise Identity Mapping.

**sniffing (čmuchání)**
Praxe monitorování nebo odposlouchávání elektronických přenosů. Informace, které se posílají po Internetu, mohou někdy projít řadou směrovačů, než se dostanou na místo určení. Výrobci směrovačů, poskytovatelé služeb sítě Internet a vývojáři operačních systémů se velmi snažili zajistit, aby v páteřní síti Internetu nemohlo ke čmuchání dojít. Výskyt úspěšného čmuchání je stále vzácnější. Většinou se vyskytne spíše v soukromých sítích LAN, které jsou napojeny na Internet, než na samotné páteřní síti. Musíte si však být vědomi možnosti čmuchání proto, že většina přenosů TCP/IP zašifrována není.

**SOCKS**
Je architektura klient/server, která přenáší provoz TCP/IP zabezpečenou branou. Server SOCKS provádí mnoho stejných služeb jako proxy server.

**spoofing (vylákání)**
Vetřelci se maskují jako důvěryhodný systém a snaží se vás přesvědčit, abyste jim zaslali utajované informace.

**T**

**TCP/IP**

Primární komunikační protokol, který se používá v síti Internet. TCP/IP je zkratka vytvořená z počátečních písmen Transmission Control Protocol/Internet Protocol. Protokol TCP/IP můžete použít také ve vaší interní síti.

**Trojan horse (trojský kůň)**

Počítačový program, příkaz nebo skript, který zdánlivě provádí užitečnou a nevinnou funkci. Obsahuje však skryté funkce, které používají schválená oprávnění přiřazená uživatelům, když program spustí. Například mohou zkopírovat interní informace o oprávnění z vašeho počítače a odeslat je zpět původci trojského koně.

**U**

**V**

**virtual private network (VPN)**

Rozšíření soukromé vnitropodnikové sítě podniku. Můžete ji použít ve veřejné síti, jako například v síti Internet, a vytvořit zabezpečené vlastní připojení, v podstatě soukromý ″tunel″. VPN bezpečně předávají informace přes Internet a připojují další uživatele k vašemu systému. Patří mezi ně:

- Vzdálení uživatelé.
- Pobočky úřadů.
- Obchodní partneři a dodavatelé.

**W**

**Web browser (prohlížeč WWW)**

Aplikace protokolu HTTP typu klient. Prohlížeč WWW interpretuje HTML a zobrazuje uživateli hypertextové dokumenty. Uživatel má přístup k objektu připojenému prostřednictvím hypertextového odkazu tak, že klepne na oblast aktuálního dokumentu (provede výběr). Tato oblast se často nazývá **aktivní bod**. Příkladem prohlížeče WWW je Internet Connection Web Explorer a Netscape Navigator.

**World Wide Web (WWW)**

Síť vzájemně propojených serverů a klientů, které používají standardní formát při tvorbě dokumentů (HTML) a přístupu k nim (HTTP). Síti odkazů jak ze serveru na server, tak z dokumentu na dokument, se metaforicky říká **Web** (pavučina).

**X**

**Y**

**Z**

# Dodatek. Upozornění

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabídnout produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou momentálně dostupné ve vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba společnosti IBM. Použít lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Získání tohoto dokumentu uživateli neposkytuje licenci na tyto patenty. Písemné dotazy ohledně licencí můžete zaslat na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení společnosti IBM ve vaší zemi, nebo písemně zastoupení společnosti IBM na adrese:

IBM
World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

**Následující odstavec neplatí pro Velkou Británii a další země, ve kterých tato opatření nejsou v souladu s místními právními předpisy:** IBM POSKYTUJE TUTO PUBLIKACI " JAK JE" (AS-IS), BEZ JAKÝCHKOLI ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÉ ZÁRUKY NEPORUŠOVÁNÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řády některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk v určitých transakcích a proto se na Vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoli odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoliv informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv závazků vůči vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

| IBM Corporation
| Software Interoperability Coordinator, Department YBWA
| 3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

IBM poskytuje licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě IBM na programy nebo v jiné ekvivalentní smlouvě.

Všechna zde obsažená data týkající se výkonu byla zjištěna v řízeném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou významně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a nelze tedy zaručit, že tato měření budou ve všeobecně dostupných systémech stejná. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by měli ověřit příslušná data pro své specifické prostředí.

Informace týkající se produktů jiných společností byly získány od dodavatelů těchto produktů, z jejich tištěných materiálů nebo z jiných veřejně dostupných zdrojů. IBM nezkoumala tyto produkty a nemůže tudíž potvrdit spolehlivost, kompatibilitu a další konstatování, vztahující se k těmto produktům. Dotazy na možnosti produktů pocházejících z jiného zdroje než od IBM adresujte dodavatelům těchto produktů.

Všechna tvrzení o budoucím zaměření nebo úmyslech IBM mohou být bez upozornění změněna nebo zrušena a představují pouze hrubý nástin cílů a podmínek společnosti.

Všechny uvedené ceny IBM jsou navrhovanými maloobchodními cenami IBM, jsou aktuální a podléhají změně bez předchozího upozornění. Ceny prodejců se mohou lišit.

Tyto informace jsou poskytovány pouze za účelem plánování. Informace zde poskytované se mohou změnit dříve, než budou popisované produkty k dispozici.

Informace obsahují příklady dat a zpráv, které jsou běžně používány v denních obchodních činnostech. Příklady obsahují jména a názvy osob, společností, značek a produktů, aby bylo možno je vysvětlit v plném rozsahu. Všechna tato jména a názvy jsou zcela fiktivní a jakákoliv podobnost se jmény či adresami existujících společností je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyce, které ilustrují programovací techniky na různých provozních platformách. Jste oprávněni bezplatně kopírovat, modifikovat a distribuovat tyto vzorové programy v jakékoliv formě, a to pro účely vývoje, užívání, marketingu nebo distribuce aplikačních programů vhodných pro rozhraní API pro operační platformu, pro kterou byly vzorové programy napsány. Uvedené příklady nebyly důkladně testovány za všech podmínek. IBM proto nemůže zaručit nebo potvrdit spolehlivost, obsluhovatelnost nebo funkčnost těchto produktů.

Každá kopie nebo část těchto vzorových programů nebo práce z nich odvozené musí zahrnovat následující copyrightovou výhradu:

© (jméno Vaší společnosti) (rok). Části tohoto kódu jsou odvozeny od vzorových programů od IBM Corporation. © Copyright IBM Corp. _zadejte rok nebo roky_. Všechna práva vyhrazena.

Pokud si tyto informace prohlížíte ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

## Ochranné známky

Následující výrazy jsou ochrannými známkami IBM v USA a případně v dalších jiných zemích:

| AIX
| AIX 5L
| e(logo) server
| eServer
| i5/OS
| IBM
| iSeries
| pSeries
| xSeries
| zSeries

| Intel, Intel Inside (loga), MMX a Pentium jsou ochranné známky společnosti Intel Corporation ve Spojených státech
| a případně v dalších jiných zemích.

Microsoft, Windows, Windows NT a logo Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

Java a všechny ochranné známky obsahující slovo Java jsou ochrannými známkami společnosti Sun Microsystems, Inc. ve Spojených státech a případně v dalších jiných zemích.

| Linux je ochranná známka, jejímž majitelem je Linus Torvalds, ve Spojených státech a případně v dalších jiných
| zemích.

UNIX je registrovaná ochranná známka společnosti The Open Group ve Spojených státech a případně v dalších jiných zemích.

Další jména společností, produktů nebo služeb mohou být ochrannými známkami jiných společností.

## Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

**Osobní použití:** Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

**Komerční použití:** Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoliv informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO ZÁRUKY VHODNOSTI PRO URČITÝ ÚČEL.

Vytištěno v  Dánsku společností IBM Danmark A/S.