IBM SecureWay FirstSecure

Pianificazione e integrazione

Versione 2

IBM SecureWay FirstSecure

Pianificazione e integrazione

Versione 2

Nota

Prima di utilizzare questa documentazione ed il relativo programma, leggere le informazioni generali contenute nell'Appendice A, “Informazioni particolari” a pagina 99.

Prima edizione (ottobre 1999)

Questa edizione fa riferimento a IBM SecureWay FirstSecure Versione 2 e a tutti i release e modifiche successivi salvo diversamente specificato nelle nuove edizioni.

Indice

Figure

Tabelle

Informazioni sul manuale

IBM SecureWay FirstSecure, noto anche come FirstSecure, è una struttura che consente di ottenere i seguenti risultati nella propria azienda:

- Rendere sicure le elaborazioni eseguite sul Web o su altre reti.
- Incrementare i propri investimenti e-business. Le offerte modulari consentono di aggiungere sicurezza in una disposizione pianificata.
- Ridurre il costo totale di possesso per l'esecuzione di e-business sicuri.

In questo manuale viene descritto FirstSecure, e i prodotti che lo costituiscono. In tal modo, l'utente viene avviato all'utilizzo di questi prodotti.

I prodotti descritti in questo manuale sono parte di un release a stadi. E' possibile che non tutti i prodotti siano disponibili nello stesso momento o in tutti i paesi. Per informazioni sulla disponibilità dei prodotti, rivolgersi ad un rappresentante commerciale IBM.

Figure contenute nel manuale

Le figure di questo manuale sono esclusivamente per la pianificazione. Ogni figura illustra solo una delle possibili configurazioni di server, client ed applicazioni che l'utente può utilizzare nella propria azienda.

Il formato delle figure dipende dal formato del manuale:

- La maggior parte delle figure nella versione PDF (Portable Document Format) del manuale sono più semplici da utilizzare, poiché non occupano molto spazio su disco ed è possibile stamparle rapidamente.
- Le figure nella versione stampata sono più complesse, richiedono una maggiore quantità di spazio su disco e tempi di stampa più lunghi.

Le figure in entrambe le figure sono funzionalmente equivalenti e presentano le medesime didascalie.

A chi è destinato il manuale

Questo manuale è destinato ai responsabili di sistema che desiderano pianificare ed integrare la sicurezza per i sistemi basati sul Web. Si suppone che l'utente abbia familiarità con le attività di rete e con le applicazioni e-business.

Organizzazione del manuale

Il manuale si compone delle seguenti sezioni:

- Parte 1, “Panoramica di FirstSecure” a pagina 1 fornisce una panoramica su FirstSecure, i relativi prodotti e le offerte disponibili.
- Parte 2, “Pianificazione di una rete e-business sicura” a pagina 15 descrive la pianificazione di una rete e-business sicura.
- Parte 3, “Considerazioni sull'installazione e sull'integrazione” a pagina 53 descrive i requisiti di installazione e fornisce informazioni sull'integrazione dei prodotti FirstSecure.
- Capitolo 16, “Documentazione fornita con FirstSecure” a pagina 87 descrive la documentazione disponibile con FirstSecure.
- “Glossario” a pagina 103 definisce i termini relativi alla sicurezza utilizzati nel manuale.

Il manuale contiene inoltre una bibliografia relativa alla documentazione di ciascun prodotto .

Anno 2000

Nelle seguenti sezioni viene descritta la compatibilità di IBM SecureWay FirstSecure con l'anno 2000.

Prodotti IBM in IBM SecureWay FirstSecure

Questi prodotti sono pronti per l'anno 2000. Quando utilizzati attenendosi alla documentazione allegata, sono in grado di elaborare, fornire e ricevere i dati sulle date comprese tra il ventesimo ed il ventunesimo secolo in modo corretto, sempre che tutti i prodotti (hardware, software e firmware) utilizzati con i prodotti, siano in grado di scambiarsi i dati relativi alle date in modo appropriato.

Altri prodotti di fornitori

Questi prodotti hanno dimostrato alla IBM che sono pronti per il 2000. Tuttavia, IBM non fornisce alcuna dimostrazione o garanzia della conformità di questi prodotti all'anno 2000. Contattare la casa produttrice per le domande concernenti la conformità all'anno 2000 di questi prodotti. Le informazioni relative a prodotti e servizi non IBM sono "ripubblicazioni" di informazioni fornite da altre società relative ai prodotti e servizi che offrono. Esse hanno dimostrato alla IBM che i prodotti sono pronti per l'anno 2000. Tuttavia, IBM non fornisce alcuna dimostrazione o garanzia della conformità di questi prodotti all'anno 2000. Contattare le case produttrici per le domande concernenti la conformità all'anno 2000 di questi prodotti. La IBM non ha verificato indipendentemente i contenuti di queste ripubblicazioni e non si assume alcuna responsabilità riguardo alla accuratezza e completezza delle informazioni in esse contenute.

Assistenza e manutenzione

Contattare la IBM per l'assistenza e la manutenzione di tutti i prodotti inclusi nell'offerta SecureWay FirstSecure. Alcuni di questi prodotti fanno riferimento ad assistenze non IBM. Se questi prodotti vengono ricevuti come parte dell'offerta SecureWay FirstSecure, rivolgersi alla IBM per ricevere assistenza.

Convenzioni

In questo manuale vengono utilizzate le seguenti convenzioni tipografiche:

- **Il testo in grassetto** indica il nome di un argomento selezionato, il nome di un comando o testo che un utente digita oppure un esempio di testo in esecuzione.
- `Il testo in carattere monospace` indica un esempio (ad esempio un percorso o nome file fittizio) o il testo visualizzato sullo schermo.

Informazioni sul Web

Le informazioni relative agli ultimi aggiornamenti di FirstSecure sono disponibili presso la pagina di Internet www.software.ibm.com/software/security ai seguenti indirizzi:

IBM SecureWay FirstSecure
www.ibm.com/software/security/firstsecure

La documentazione è disponibile all'indirizzo
www.ibm.com/software/security/firstsecure/library

IBM SecureWay Policy Director
www.ibm.com/software/security/policy

La documentazione è disponibile all'indirizzo
www.ibm.com/software/security/policy/library

IBM SecureWay Boundary Server
www.ibm.com/software/boundary

La documentazione è disponibile all'indirizzo
www.ibm.com/software/boundary/library

IBM SecureWay Trust Authority
www.ibm.com/software/security/trust

La documentazione è disponibile all'indirizzo
www.ibm.com/software/securitytrust/library

Un Redbook ITSO, *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498–00 è disponibile all'indirizzo Internet www.ibm.com/redbooks.

Parte 1. Panoramica di FirstSecure

In questa sezione viene fornita una panoramica di FirstSecure e dei relativi prodotti. Contiene una breve descrizione di ciascun prodotto.

Contiene inoltre informazioni sui servizi di implementazione IBM.

Capitolo 1. Descrizione di FirstSecure

IBM SecureWay FirstSecure fa parte delle soluzioni di sicurezza integrata della IBM. FirstSecure è una serie completa di parti componibili che sono di ausilio per le società nell'esecuzione delle operazioni seguenti:

- Stabilire un ambiente e-business sicuro.
- Ridurre i costi legati alla sicurezza, semplificandone la pianificazione.
- Realizzare politiche di sicurezza più facilmente.
- Creare un ambiente e-business più efficace.

I componenti di FirstSecure forniscono la protezione da virus, l'individuazione di intrusi, il controllo degli accessi e del tipo di traffico, la cifratura e i certificati digitali. Queste funzioni sono fornite dalla famiglia IBM SecureWay di prodotti per la sicurezza oppure da offerte di altri fornitori, combinando quindi i migliori componenti di diversi fornitori di sicurezza. Inoltre, sono disponibili dei Servizi di implementazione per alcuni componenti FirstSecure. I blocchi di creazione di FirstSecure sono:

- SecureWay Policy Director
- SecureWay Boundary Server
- Intrusion Immunity
- Public Key Infrastructure, fornito mediante IBM SecureWay Trust Authority
- IBM SecureWay Toolbox

Poiché FirstSecure è costituito da una serie di prodotti che possono essere installati in maniera indipendente, è possibile creare un ambiente sicuro. L'utente può partire da una determinata area, verificare i miglioramenti e ricercare un contesto di maggiore sicurezza. Ciò riduce complessità e i costi e consente lo sviluppo di risorse e di applicazioni Web.

Perché utilizzare FirstSecure

I propri dati e le proprie risorse sono vitali per e-business. I prodotti di FirstSecure forniscono:

Autorizzazione

Ognuno deve attenersi alle regole. Mediante le autorizzazioni solo determinati utenti possono accedere al proprio sistema, ai propri dati, alle proprie applicazioni e reti.

Responsabilità
E' possibile determinare chi ha eseguito cosa e quando. La responsabilità consente di determinare chi ha eseguito una determinata azione e quali azioni sono state eseguite durante un determinato intervallo di tempo.

Garanzia
Il sistema è in grado di soddisfare le richieste di sicurezza. In tal modo, viene garantita l'applicazione del livello di sicurezza richiesto.

Disponibilità
Il sistema può essere utilizzato dall'utente in qualsiasi momento. In tal modo, i sistemi, i dati, le reti e le applicazioni possono essere utilizzati dai propri impiegati, fornitori, partner e clienti.

Gestione
L'utente può definire le regole. Ciò consente di definire, conservare, controllare e modificare le informazioni sulla politica utilizzata.

L'utente può realizzare questo livello di protezione in base a politiche di ampio raggio che consente di proteggere le reti, i sistemi e le applicazioni della propria azienda. La presenza di un collegamento vulnerabile tra i prodotti inseriti nella rete di protezione inficia l'intera infrastruttura.

Questo manuale inserisce ciascun prodotto del blocco di creazione di SecureWay nell'elenco delle protezioni fornite.

Definizione dei blocchi di creazione di FirstSecure

FirstSecure contiene i prodotti del componente che è possibile richiedere in un unico gruppo o separatamente. Questi prodotti possono disporre di uno o più prodotti del componente. E' possibile cominciare con qualsiasi prodotto e creare una soluzione di sicurezza completa.

Policy Director

Policy Director è l'elemento centrale della pianificazione della sicurezza. Policy Director fornisce l'autorizzazione e la gestione della sicurezza end-to-end delle risorse Web su reti interne ed esterne. Policy Director fornisce l'autentica, l'autorizzazione, la sicurezza dei dati e la gestione delle risorse. Policy Director, utilizzato insieme alle tradizionali applicazioni basate su Internet consente di creare delle intranet sicure e ben gestite. Policy Director include:

- Security Services

- Management Console
- Management server
- Security Manager (NetSEAL e WebSEAL)
- NetSEAT client
- Directory Services Broker
- Authorization server (supporto applicazioni terze parti)

Policy Director viene eseguito in Windows NT, AIX e Solaris.

Per una descrizione più dettagliata di Policy Director, consultare il capitolo Capitolo 5, “Pianificazione di Policy Director nella propria rete” a pagina 31.

SecureWay Boundary Server

I prodotti di SecureWay Boundary Server forniscono la garanzia, la gestione e la responsabilità per le applicazioni e-business basate sul Web. Le barriere di protezione sono necessarie ovunque—tra i reparti, ad esempio ingegneria e risorse umane, tra le reti degli uffici centrali e gli uffici distaccati, tra la rete della propria azienda e Internet, tra le applicazioni Web della propria azienda e i clienti, infine tra la rete della propria azienda e i propri partner commerciali. Porre delle barriere di sicurezza significa controllare coloro che accedono alla rete e le informazioni che vengono inoltrate su di essa.

In questa sezione vengono descritti i blocchi di creazione di SecureWay Boundary Server. Per informazioni sulla pianificazione e l'integrazione, consultare il Capitolo 12, “SecureWay Boundary Server - Requisiti e considerazioni sull'installazione” a pagina 59.

IBM SecureWay Firewall

IBM SecureWay Firewall, denominato anche IBM Firewall, abilita transazioni e-business protetti e sicuri, controllando tutte le comunicazioni Internet. IBM Firewall contiene tre funzioni firewall principali — filtraggio, proxy e gateway a livello di circuito — per fornire agli utenti un livello elevato di sicurezza e flessibilità.

ACE/Server

ACE/Server, da Security Dynamic, include token SecurID (2 licenze utente e 2 token). ACE/Server aggiunge un collegamento per il responsabile e un collegamento *VPN (virtual private network)* al IBM SecureWay Firewall.

MIMEsweeper per IBM SecureWay Rilascio 2

MIMEsweeper, da Content Technology, include i componenti per Internet security. MAILsweeper controlla i messaggi per verificare che nessuna comunicazione confidenziale lasci l'ambiente e-business e che nessun messaggio non autorizzato vi acceda.

WEBsweeper impedisce l'accesso al proprio ambiente e-business di materiale Web non desiderato. Analizza e accetta i dati solo da applet Java autorizzate, codici eseguibili o siti Web.

SurfinGate

SurfinGate, di Finjan Software Ltd., è una soluzione di sicurezza a codice mobile per e-business. Poichè il codice mobile ì attualmente inserito e instradato automaticamente dall'esterno della rete Intranet, nella rete e-business, è necessaria una protezione più' elevata rispetto a quella fornita dai firewall. SurfinGate protegge la rete da attacchi da parte di codici Java, ActiveX e JavaScript. Identifica eventuali attacchi, li allontana dalle risorse critiche prima del loro ingresso nella rete. Isola i dati sospetti in modo che l'utente possa esaminarli prima di accettarli.

Intrusion Immunity

Intrusion Immunity fornisce un'assicurazione nella forma di prodotti di protezione e rilevazione per le imprese. Per informazioni sui requisiti di Intrusion Immunity, consultare il Capitolo 13, “Intrusion Immunity - Requisiti e considerazioni sull'installazione” a pagina 67. Intrusion Immunity include Tivoli Cross-Site for Security e Norton AntiVirus.

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security consente di individuare i dati non desiderati in sistemi vulnerabili. Tivoli Cross-Site for Security consente di:

- Installare nella propria rete gli agenti Cross-Site for Security per notificare eventuali situazioni sospette.
- Prendere visione dei dati non desiderati in prospetti predefiniti e personalizzati.
- Individuare e registrare attività non autorizzate o sospette in tempo reale.
- Regolare gli agenti di sicurezza per ridurre il numero di falsi allarmi.

Norton AntiVirus

Norton AntiVirus, un prodotto della Symantec Corporation, è uno dei prodotti software antivirus più diffuso nel mondo. Norton AntiVirus può essere eseguito costantemente sullo sfondo in modo che i computer siano sempre protetti dai virus che potrebbero accedere mediante la posta elettronica, i controlli ActiveX, le applet Java, gli scaricamenti di programmi da Internet, minidischi, CD dei software o mediante i file inviati sulla rete. Norton AntiVirus consente di isolare i file infetti. E' possibile configurare Norton AntiVirus per aggiornare automaticamente l'utente sui nuovi virus.

Public Key Infrastructure

IBM FirstSecure supporta gli standard PKI (Public Key Infrastructure) per la cifratura e l'interoperabilità mediante IBM SecureWay Trust Authority.

SecureWay Trust Authority è una soluzione che supporta l'emissione, il rinnovo e la revoca di certificati digitali. Questi certificati possono essere utilizzati in un'ampia gamma di applicazioni Internet. Essi consentono l'autentica degli utenti e garantiscono la sicurezza delle informazioni. Trust Authority è basato sulle specifiche del gruppo di lavoro PKI *Public Key Infrastructure* di *IETF (Internet Engineering Task Force)*. Comprende:

- Supporto per i server IBM AIX e Microsoft Windows NT
- Una RA (registration authority)
- Una CA (certificate authority)
- Delle interfacce utente per la richiesta di certificati e la gestione di quelli emessi.
- Un *IBM SecureWay Directory* integrato
- Un sistema secondario di *audit*
- Supporto per coprocessore di cifratura SecureWay 4758
- Supporto per *schede intelligenti*

Questa infrastruttura copre l'intero ciclo di vita dei certificati, inclusi l'iscrizione e la certificazione iniziale, l'aggiornamento delle coppie di chiavi, il rinnovo dei certificati, la pubblicazione di elenchi di certificati e di revoche di certificati e la revoca di certificati. Per ulteriori informazioni, consultare l'Capitolo 14, “Public Key Infrastructure - Requisiti e considerazioni sull'installazione” a pagina 75.

Toolbox

FirstSecure Toolbox è costituito da una serie di toolkit per la sicurezza che sono parte di o interagiscono con i principali componenti di FirstSecure. I toolkit consentono di:

- Integrare le applicazioni con FirstSecure.

- Personalizzare le soluzioni e le applicazioni mediante FirstSecure.
- Creare applicazioni ISV e OEM che utilizzano FirstSecure.

Le API dei toolkit di FirstSecure Toolbox supportano le seguenti funzioni di sicurezza:

- Servizi relativi alle autorizzazioni
- Servizi relativi ai certificati e alla gestione
- Servizi di Directory
- Servizi di protocollo Secure Sockets Layer
- Servizi di gestione cifratura e sicurezza KeyWorks
  - API di IBM Key Recovery Service Provider 1.1.3.0 . IBM Key Recovery Service Provider consente di recuperare le informazioni cifrate.
  - IBM Key Recovery Server 1.1.3.0. IBM Key Recovery Server 1.1.3.0 è un'applicazione che sulla base di una richiesta autorizzata consente di recuperare le informazioni cifrate se le chiavi non sono disponibili, se sono perse o danneggiate.

    Questi due toolkit forniscono delle interfacce standard che possono essere utilizzate dalle applicazioni per richiamare i servizi di sicurezza critici e dai fornitori della sicurezza per utilizzare il toolkit. Le interfacce standard si basano sull'architettura CDSA (Common Data Security Architecture). Questi toolkit sono disponibili in Windows NT, Solaris e AIX.

Servizi di implementazione

I servizi di implementazione di FirstSecure consentono ad e-business di avviare FirstSecure rapidamente ed in modo efficace. Questi servizi, che possono essere acquistati separatamente, sono forniti dalla IBM e sono eseguiti da un gruppo di consulenti esperti. I servizi di implementazione di FirstSecure comprendono FirstSecure Implementation Workshop e servizi di installazione QuickStart. La IBM può inoltre fornire servizi di integrazione di sistema di FirstSecure personalizzati per il proprio ambiente.

Per informazioni, rivolgersi ad un rappresentante commerciale IBM.

Capitolo 2. Novità del Rilascio 2

Nel rilascio 2 vengono semplificate la pianificazione e l'installazione dei prodotti di IBM SecureWay FirstSecure. I singoli prodotti sono più integrati, sono stati aggiunti dei prodotti e la gestione e il controllo sono stati maggiormente centralizzati.

Policy Director

Policy Director presenta le seguenti nuove funzioni:

- Il supporto per IBM SecureWay Directory per la memorizzazione delle informazioni sulle credenziali di utenti e gruppi.
- Gli ultimi aggiornamenti alle specifiche delle API delle autorizzazioni da Open Group.
- La possibilità di definire e di editare le credenziali dell'utente del proxy di IBM Firewall mediante Management Console di Policy Director.
- Un servizio CAS (Credentials Acquisition Service) di Policy Director che fornisce il supporto per l'utilizzo di servizi di autentica esterni.
- Il supporto per l'autentica del client basata sui certificati mediante il nuovo servizio CAS di Policy Director.
- La possibilità di scrivere il proprio servizio di acquisizione di credenziali personalizzato mediante l'interfaccia IDL (Interface Definition Language) tra WebSEAL e il servizio CAS di Policy Director. Policy Director fornisce inoltre un server generale che gestisce le funzioni server del servizio CAS di Policy Director, ad esempio l'avviamento, la registrazione del server e la gestione dei segnali.
- La possibilità di utilizzare un meccanismo di regolazione di SSL (secure sockets layer) in aggiunta alla regolazione dei servizi GSS (generic security services).
- L'utilizzo di Management Console di Policy Director, o l'interfaccia della riga comandi per gestire le politiche relative ai collegamenti e alle password.
- L'utilizzo di Management Console di Policy Director, o l'interfaccia della riga comandi per gestire la registrazione di singoli utenti, di gruppi o di risorse (destinazioni).
- Uno strumento di gestione delle password per la registrazione di una singola destinazione basato sul Web.
- Un processo di installazione integrato.

SecureWay Boundary Server

SecureWay Boundary Server presenta le seguenti nuove funzioni:

- Una GUI di configurazione che unisce alcune funzioni di SecureWay Boundary Server e di Policy Director.
- Una nuova TaskGuide di configurazione che unisce alcune funzioni di SecureWay Boundary Server e di Policy Director.

Novità in IBM SecureWay Firewall per AIX e NT

IBM SecureWay Firewall, noto anche come IBM Firewall, presenta le seguenti nuove funzioni:

Funzioni sicure per il proxy di posta

IBM Firewall Secure Mail Proxy presenta le seguenti nuove funzioni:

- Algoritmi anti-SPAM inclusi il blocco di messaggi provenienti da spammer noti (un elenco di esclusione), controlli della validità e della possibilità di rispondere ai messaggi (metodi noti per bloccare messaggi non desiderati), limiti configurabili del numero di destinatari dei messaggi di posta e delle dimensioni massime di un messaggio.
- Supporto contro gli inganni che interagisce con i meccanismi di autentica
- Supporto per errori SNMP e per MADMAN MIB
- Funzione di traccia TraMessage inclusa la possibilità di eseguire la traccia dei messaggi tra firewall e Domino senza interruzioni

Miglioramenti del protocollo Socks versione 5

Il protocollo Socks versione 5 è stato aggiornato per includere le autentiche UNPH (username-password), CRAM (challenge/response) e i plug-in per le autentiche.

Il collegamento è stato migliorato per fornire all'utente un maggiore controllo nella classificazione dei messaggi di registrazione e nella specifica dei livelli di registrazione.

Proxy HTTP

IBM SecureWay Firewall fornisce un proxy HTTP basato sul prodotto IBM WTE (Web Traffic Express). Il proxy HTTP gestisce in maniera ottimale le richieste del browser mediante IBM Firewall, eliminando la necessità di server socks per l'utilizzo di browser Web. Gli utenti possono accedere alle

informazioni su Internet, senza compromettere la sicurezza delle proprie reti interne e senza dover alterare l'ambiente client per avvalersi di un proxy HTTP.

RAS (Remote Access Service)

Windows NT RAS (Remote Access Service) fornisce connessioni di rete mediante supporti dial-up, ISDN o X.25, utilizzando il protocollo PPP (Point-to-Point Protocol). NDISWAN è un driver di rete fornito come parte del servizio RAS. Converte i dati PPP sottostanti in modo che somiglino ai dati Ethernet LAN.

Nuove funzioni di IBM SecureWay Firewall per AIX

IBM SecureWay Firewall per AIX offre numerose nuove funzioni:

Supporto IPSec avanzato

Il supporto IPSec avanzato include il supporto per nuove intestazioni. Supporta inoltre l'interoperabilità con svariati server e router IBM e con molti prodotti VPN non IBM che supportano le nuove intestazioni.

Supporto MP (Multi-Processor)

Gli utenti di Firewall possono utilizzare le funzioni multiprocessore del sistema RS/6000 per migliorare le prestazioni.

Miglioramenti dei filtri

Migliori prestazioni e maggiore flessibilità con la configurazione. E' possibile regolare le prestazioni del IBM SecureWay Firewall scegliendo dove collocare i diversi tipi di regole di filtraggio. Un indicatore di filtraggio indica quante volte viene utilizzata una connessione.

Conversione dell'indirizzo di rete

Supporto corrispondenza di molti indirizzi con un solo indirizzo Queste corrispondenze vengono stabilite tra più indirizzi interni non registrati o privati e un indirizzo legale registrato, utilizzando dei numeri di porta per creare delle corrispondenze univoche.

Procedura guidata di configurazione

Nei passi iniziali della configurazione di IBM Firewall viene utilizzata una procedura guidata. La procedura guidata consente agli utenti con poca

familiarità con il IBM Firewall di eseguire rapidamente la configurazione in seguito all'installazione.

NSA (Network Security Auditor)

NSA (Network Security Auditor) verifica i server della rete e il IBM Firewall per individuare eventuali problemi di sicurezza o errori di configurazione. E' uno strumento più rapido ed efficace.

Novità in MIMEsweeper per IBM SecureWay Rilascio 2

Le nuove funzioni di MAILsweeper includono:

- La rilevazione delle parole chiave per bloccare i messaggi di posta elettronica fastidiosi o diffamatori e per fare in modo che i dati riservati non escano dalla società
- Blocco di posta pubblicitaria non desiderata
- Impedire ad individui o gruppi di inviare o ricevere determinati tipi di file
- Bloccare o ritardare la ricezione dei file in base alle dimensioni per evitare eccessivo traffico sulla rete

Le nuove funzioni di WEBsweeper includono:

- Impedire agli impiegati di accedere a determinati siti non legati alle attività lavorative.
- Impedire gli attacchi per estrarre documenti mediante HTML o gli indirizzi E-mail e le informazioni sul sito mediante cooky.

Novità in SurfinGate

SurfinGate presenta le seguenti nuove funzioni:

- Controllo del contenuto JavaScript
- Controllo delle prestazioni mission-critical
- Gestione delle politiche incrementata
- Supporto per i protocolli FTP (File Transfer Protocol) e HTTPS
- Integrazione plug-in con il proxy HTTP del firewall
- La capacità di bloccare lo scaricamento di specifici file eseguibili in un computer di un utente

Intrusion Immunity

I prodotti Intrusion Immunity comprendono Tivoli Cross-Site for Security.

Novità in Tivoli Cross-Site for Security

Tivoli Cross-Site for Security consente di individuare eventuali dati non desiderati. Consente di monitorare gli attacchi alla rete che compromettono l'integrità dell'ambiente e-business

Novità in Norton AntiVirus Solution Suite

Norton AntiVirus Solution Suite, Rilascio 3.0.4, include le seguenti versioni aggiornate:

- Norton AntiVirus 5.02 per Windows 95/98 e Windows NT Workstation
- Norton AntiVirus 5.02 per Windows NT Server
- Norton AntiVirus per IBM Operating System/2 (OS/2) 5.02
- Norton AntiVirus OS/2 per Lotus Notes 2.0
- Norton AntiVirus per Lotus Notes 2.0
- Norton AntiVirus per Microsoft Exchange 1.5.2

Public Key Infrastructure

Il componente di Public Key Infrastructure include Trust Authority. Trust Authority include:

- Una procedura guidata facilita l'installazione in Windows NT.
- Una configurazione preimpostata per la scheda di cifratura 4758. L'utente può modificare queste informazioni.
- Una procedura guidata di configurazione che verifica la validità dei dati prima dell'avvio dei programmi di configurazione sullo sfondo.
- Individuazione dei messaggi di errore e relativa notifica.
- Documentazione in linea, inclusi la guida contestuale per le procedure guidate di configurazione, Registration Authority Desktop e un'applicazione client finale.

IBM SecureWay Toolbox

Toolbox presenta le seguenti nuove funzioni:

- Le API di Policy Director e la documentazione.
- Le API del Directory service.
- Le API di PKIX (Public Key Infrastructure) e la documentazione.
- IBM Key Recovery Server 1.1.3.0 è ora fornito con Toolbox. E' disponibile solo in inglese.

Parte 2. Pianificazione di una rete e-business sicura

Nella seconda sezione del manuale viene discussa la pianificazione di una rete e-business sicura.

I seguenti capitoli contengono informazioni sul traffico tipico delle comunicazioni su Internet, sui problemi di sicurezza e sul funzionamento dei prodotti FirstSecure nella propria rete e-business.

Questa sezione contiene i seguenti capitoli:

Capitolo 3. Panoramica della rete e-business

La rete e-business è costituita da una serie di risorse: dati e database, utenti, clienti, fornitori, programmatori, hardware, informazioni sulla società e così via. Verranno illustrate alcune di queste aree e verranno individuati i livelli di sicurezza richiesti.

Internet è una rete piuttosto complessa. I dati viaggiano sulla rete da un server all'altro e da un utente all'altro in percorsi non definiti che variano a seconda della trasmissione.

I propri dati vengono trasmessi su Internet insieme a quelli di tutti gli altri utenti della rete. I dati vitali per le proprie attività possono essere inoltrati attraverso qualsiasi server in un punto qualsiasi della rete. Qualunque utente di Internet può tentare di accedere alle proprie risorse, ai propri impiegati e ai propri dati. Purtroppo, insieme al traffico legittimo per l'educazione, il commercio e lo svago, Internet contiene anche traffico pericoloso, creato deliberatamente o per errore. Figura 1 a pagina 18 fornisce una panoramica dell'interazione delle proprie comunicazioni su Internet con quelle di tutti gli altri utenti.

FirstSecure consente di separare e di proteggere le proprie trasmissioni da tutte le altre.

L'utente non desidera operare in una rete Internet di questo tipo. Desidera lo scenario descritto nella Figura 2 a pagina 19, una rete Internet i cui dati sono protetti tramite FirstSecure.

Rete Internet protetta mediante FirstSecure

La maggior parte del traffico e-business passa attraverso Internet. L'utente tuttavia non desidera operare in una rete Internet che consente a quasi tutti gli utenti dotati di un computer di accedere ai propri dati. La Figura 2 a pagina 19 illustra la rete Internet che si desidera utilizzare.

Internet consente di accedere ad una serie di informazioni utili, tuttavia, è possibile che l'utente desideri separare dai propri dati aziendali alcune applicazioni, dati e accessi. Si desidera ottenere i seguenti risultati:

- Gli impiegati non vengano distratti dalle proprie attività.
- I dati degli impiegati siano protetti da messaggi inappropriati.
- Le informazioni confidenziali non vengano divulgate all'esterno.

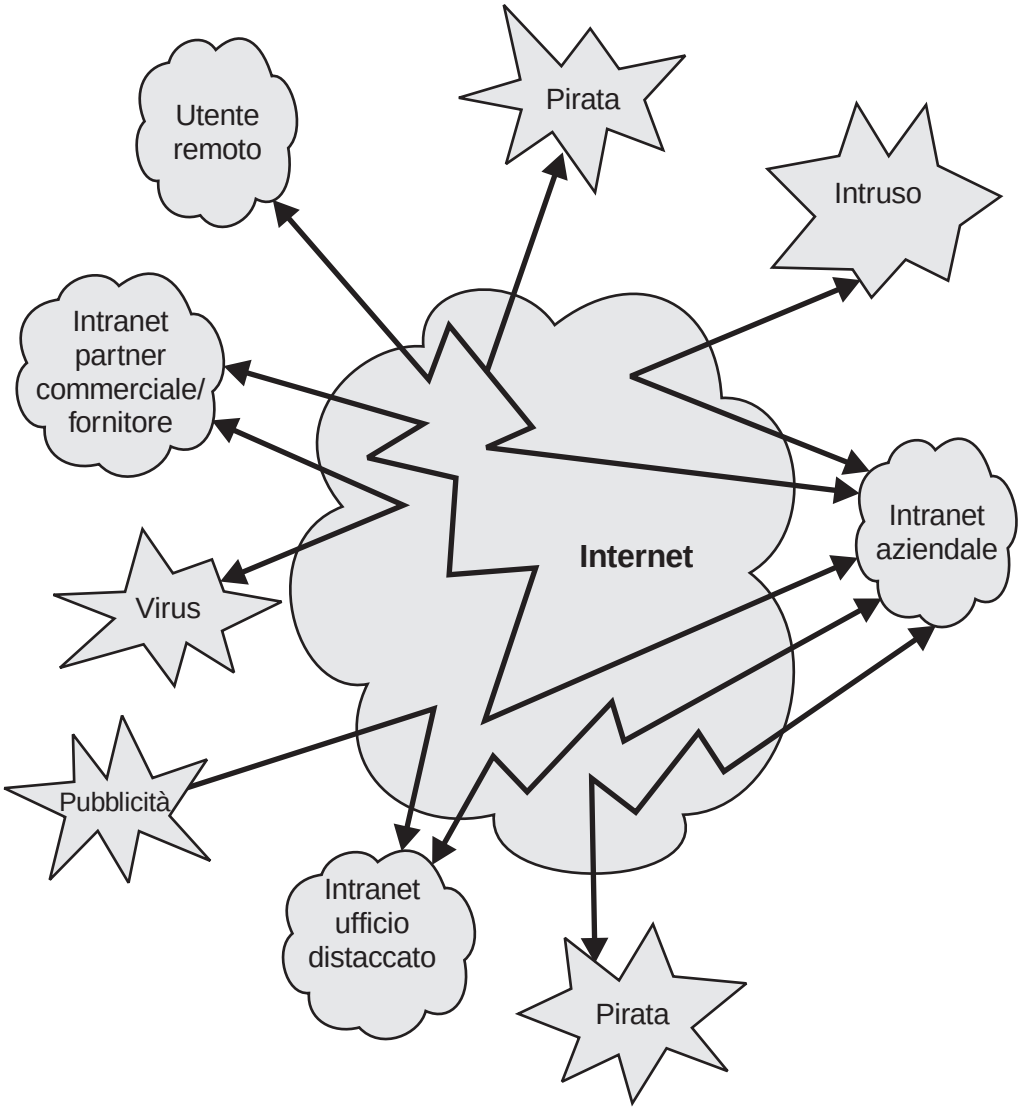


Figura 1. Panoramica del traffico di Internet con attività non correlate

VPN (Virtual Private Network)

Una rete VPN (virtual private network) identifica una connessione Internet privata, non accessibile ad altri utenti. La Figura 3 a pagina 20 illustra una tipica rete VPN. La connessione è garantita da intrusioni da parte di applicazioni o utenti non desiderati. I prodotti FirstSecure, ad esempio IBM SecureWay Firewall consentono di configurare e di supportare le reti VPN.

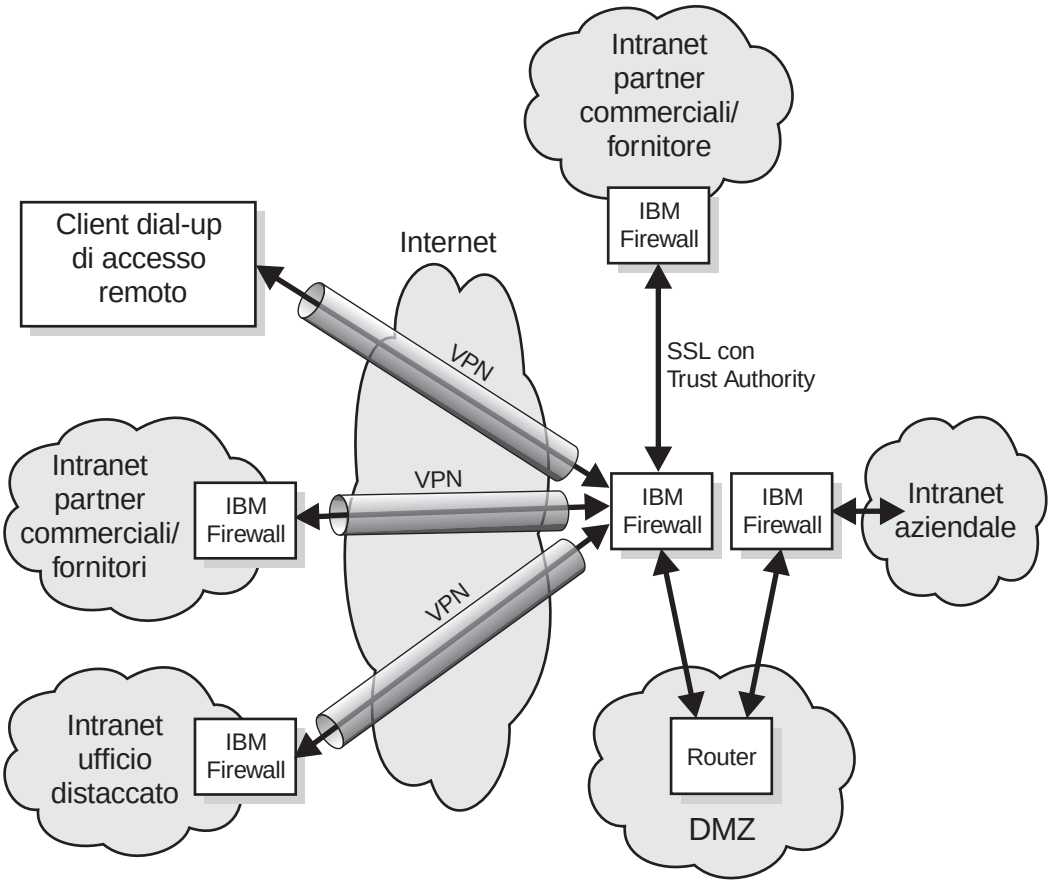


Figura 2. La rete Internet che si desidera utilizzare

DMZ (demilitarized zone)

DMZ *(demilitarized zone)* è l'insieme di risorse che consentono l'accesso agli utenti esterni. Gli utenti utilizzano IBM Firewall, MIMEsweeper e altri prodotti FirstSecure per essere certi che solo determinati utenti abbiano accesso alla zona DMZ e che essi possano accedere solo a determinate risorse. Il traffico all'interno e all'esterno della zona DMZ deve essere controllato.

Il catalogo della società può trovarsi in una zona DMZ, in modo che possa essere esaminato da potenziali clienti. Oppure è possibile avere dei prospetti informativi che descrivono la propria società. I componenti di FirstSecure consentono l'accesso alle informazioni comprese nella zona DMZ solo agli utenti autorizzati.

La Figura 4 a pagina 21 illustra una zona DMZ tipica.

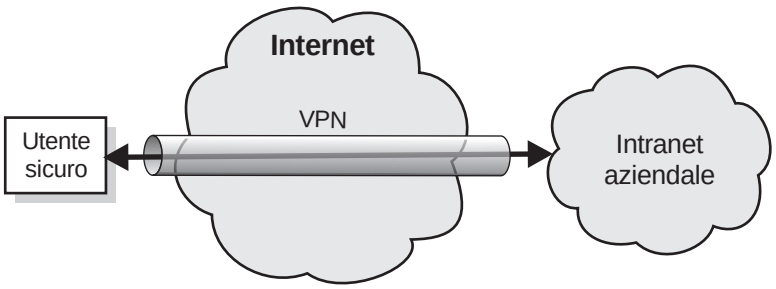


Figura 3. Una VPN (virtual private network) tipica.

Durante la creazione di applicazioni sicure è possibile utilizzare la zona DMZ per verificare la rete intranet prima di fornire gli accessi per quelle applicazioni.

Nelle seguenti sezioni verrà esaminata la tipologia di informazioni per le quali viene utilizzata la rete Internet o Intranet.

Tipica Intranet aziendale

La rete intranet aziendale è lo strumento utilizzato per comunicare all'interno di un'azienda. Contiene informazioni e risorse che non si desidera condividere con la rete Internet. Gli impiegati condividono i dati, si scambiano messaggi di posta elettronica, accedono alle risorse aziendali, quali i database, le stampanti e gli scanner. La Figura 5 a pagina 22 illustra un esempio di una rete Intranet tipica.

E' necessario fare in modo che le informazioni confidenziali siano circoscritte nell'ambito dell'azienda e che vi accedano solo utenti autorizzati. Tuttavia, si desidera fornire ai propri clienti l'accesso ad alcuni dati. Ad esempio, se si desidera che un risparmiatore sia in grado di controllare il saldo di un conto, senza che abbia accesso ai record degli impiegati. IBM Firewall garantisce la riservatezza delle informazioni private.

I prodotti di IBM FirstSecure contribuiscono alla sicurezza della propria Intranet. Policy Director consente di impostare le regole di accesso. IBM SecureWay Trust Authority provvede all'identificazione degli utenti. Tivoli Cross-Site for Security consente di individuare eventuali tentativi di accesso non autorizzato alle risorse della propria rete Intranet.

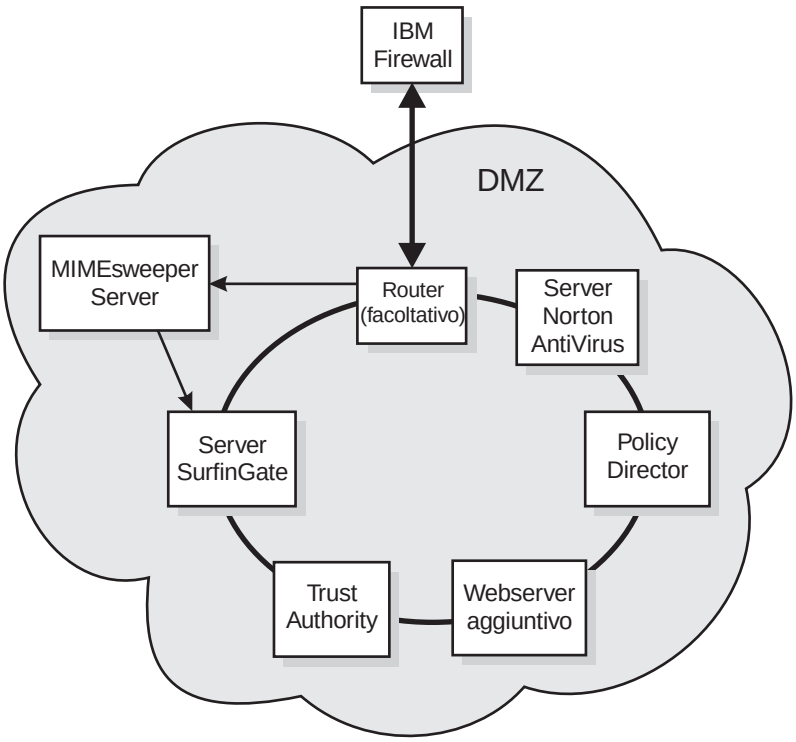


Figura 4. Zona DMZ tipica con risorse di sistema.

Tipica Intranet ufficio distaccato

Gli impiegati degli uffici distaccati devono poter accedere agli stessi dati e risorse degli impiegati della sede centrale. Le connessioni telefoniche per l'invio e la ricezione delle informazioni sono lente e non protette da interferenze esterne. Utilizzando Internet per le comunicazioni vengono ridotti i costi e viene garantita la protezione delle transazioni. La Figura 6 a pagina 23 illustra un esempio delle comunicazioni tra gli uffici distaccati e la sede centrale mediante Internet.

Si desidera garantire la stessa sicurezza della trasmissione e dei dati presente all'interno dell'azienda. La rete *VPN (virtual private network)* è il proprio canale in Internet. Gli utenti utilizzano Internet alla stregua di una rete Intranet privata.

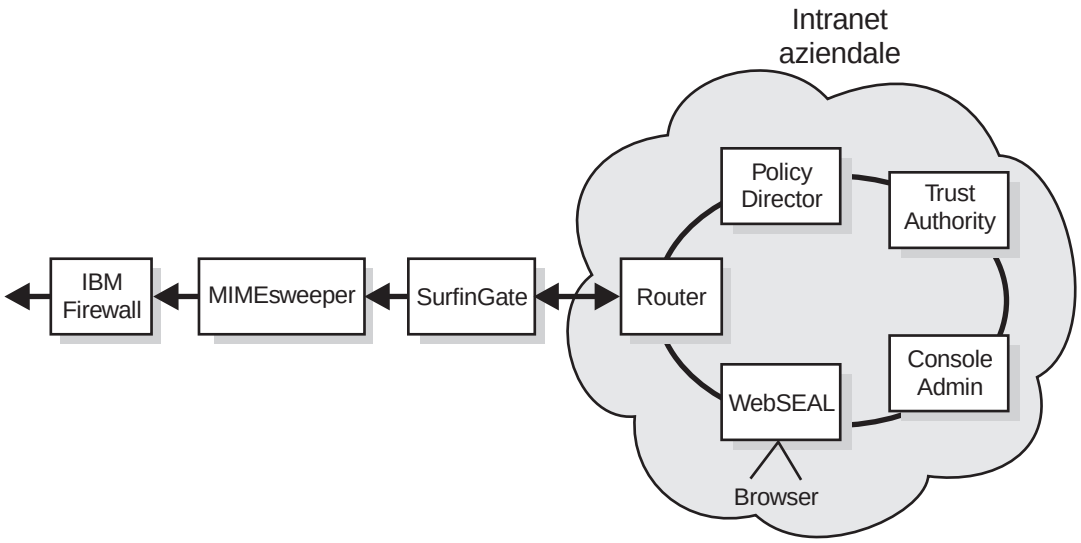


Figura 5. Panoramica di una tipica Intranet aziendale

Tipica Intranet per impiegati con accesso remoto

Alcuni impiegati possono, ad intervalli o permanentemente, lavorare in un ufficio distaccato dalla sede centrale. In tal caso, possono accedere alla rete mediante una connessione Internet di tipo dial-up o leased.

IBM Firewall protegge le trasmissioni dell'impiegato.

Intranet per partner commerciale o fornitore tipico

Una società è più efficiente se i soci in affari e i fornitori possono accedere ad alcuni dei dati della società direttamente. Un fornitore può essere autorizzato a controllare i livelli dell'inventario e ad inviare nuove scorte al raggiungimento dei livelli specificati. Un altro partner commerciale può accedere a record selezionati. Una società contabile può avere la necessità di accedere ad altri record relativi a tasse ma non ai record dei partner commerciali. Figura 8 a pagina 25 e Figura 9 a pagina 26 visualizzano un esempio tipico relativo ad un fornitore o ad un partner commerciale. Si desidera che

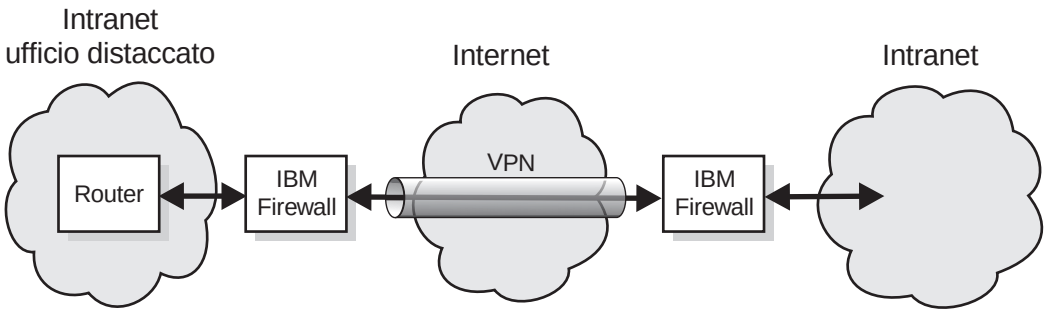


Figura 6. Ufficio distaccato collegato alla sede centrale mediante una rete VPN (virtual private network)

una transazione commerciale utilizzi Internet come se stesse viaggiando in una connessione privata.

Questo partner commerciale utilizza SSL (Secure Sockets Layer) in luogo di una rete VPN, perché le trasmissioni sono cifrate in ogni punto. L'utente può anche utilizzare una rete VPN per un ulteriore livello di sicurezza.

E' necessario proteggere gli utenti tra loro, da interferenze e da altri dati non desiderati. E' necessario proteggere la trasmissione dei dati da utenti non autorizzati. Occorre inoltre garantire che gli utenti accedano solo a determinati dati. Infine, si desidera che ciascuno di questi utenti rifletta le proprie attese.

Dati e database

I dati costituiscono le risorse più importanti all'interno di un'azienda. Alcuni dati e-business sono progettati per essere disponibili per tutti gli utenti di Internet. Ad esempio, un fornitore di hardware può rendere disponibili il proprio inventario e l'elenco dei prezzi per consentire la vendita in linea. Allo stesso modo, un commerciante di abbigliamento può rendere disponibile un catalogo illustrato di stili, colori e taglie per la vendita in linea.

Prima di fornire l'accesso ai dati, è necessario individuare il richiedente e per quale motivo vengono richiesti i dati. Trust Authority consente di emettere dei certificati per gli utenti autorizzati.

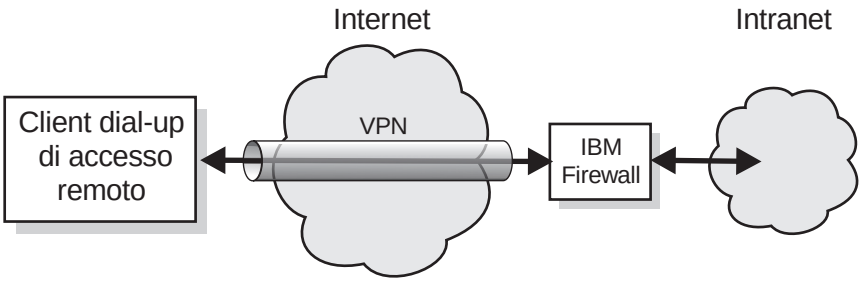


Figura 7. Client dial-up con accesso remoto collegato alla sede centrale mediante una rete VPN (virtual private network)

Altre aree da proteggere

In questo manuale non vengono indicate le contromisure per altre aree di sicurezza. Occorre pianificare quanto segue:

- Sicurezza sito, accessi, uscite e compartimentalizzazione
- Sicurezza fisica di computer portatili, personal computer, stazioni di lavoro ed altro
- Controlli in background della sicurezza personale
- Declinazioni di responsabilità legali, contratti ed affini
- Pratiche operative come ad esempio la gestione chiavi, il controllo delle informazioni e i corsi e l'apprendimento dei concetti di sicurezza

Il sistema operativo

Nella maggior parte dei casi i sistemi operativi sono configurati per l'alta disponibilità e per un'ampia gamma di funzioni. Un approccio efficace prevede di disporre solo delle funzioni necessarie a svolgere una determinata attività. Può essere utile disinstallare o disabilitare tutte le funzioni del sistema operativo, per evitare che utenti non desiderati vi accedano.

Utenti tipici

Ad Internet possono accedere diverse tipologie di utenti, non sempre desiderati. In un ambiente e-business possono accedere solo clienti che eseguono ricerche o fanno acquisti in linea. In un ambiente e-business si desidera inoltre che i partner commerciali possano accedere a determinati dati per verificare l'inventario, per prendere decisioni di produzione o per discutere dei piani e delle attività all'interno dell'azienda. Si desidera infine che gli impiegati possano accedere ai dati necessari per svolgere le attività loro assegnate.

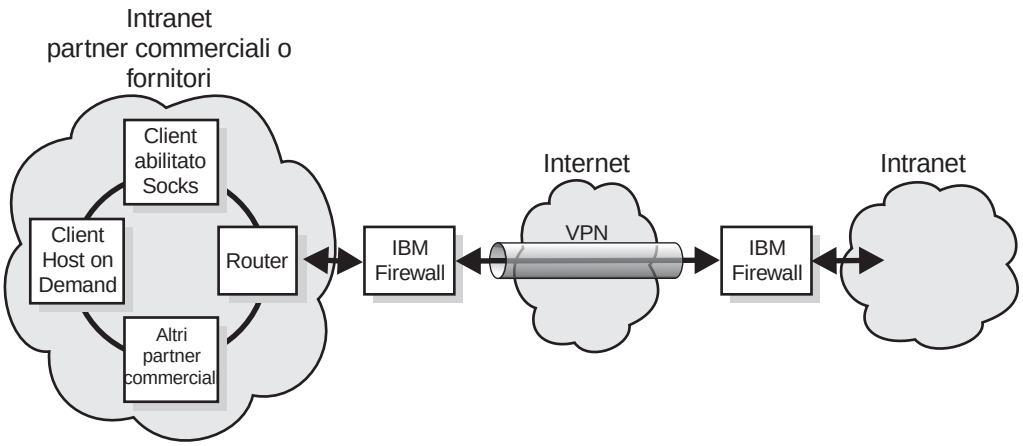


Figura 8. Intranet di un fornitore o di un partner commerciale tipico mediante una rete VPN (virtual private network)

Ad Internet possono accedere molti utenti che si desidera escludere dall'ambiente e-business: gli hacker, gli spammer, i diffusori di virus e gli utenti che desiderano accedere ai propri dati sensibili. Questi utenti possono anche esistere all'interno del proprio ambiente e-business.

Prima di concedere l'accesso alle risorse, è necessario individuare il richiedente, definire il tipo di accesso ai dati e alle applicazioni per quell'utente e quali record dell'accesso utente conservare.

Applicazioni e creazione di applicazioni

Le applicazioni possono essere progettate per includere la sicurezza. L'utente può trarre vantaggio dalla cifratura dei dati da trasmettere, dalla certificazione degli utenti che richiedono l'accesso, dall'esame delle registrazioni degli utenti e delle transazioni.

Le API di Toolbox consentono di aggiungere la sicurezza alle proprie applicazioni.

Sicurezza dell'hardware

I server e le banche dati sono parte di un sistema sicuro. Sebbene in questo manuale non vengano fornite indicazioni per l'hardware, è necessario pianificare la sicurezza fisica dei server e delle stazioni di lavoro utilizzate per la gestione della sicurezza.

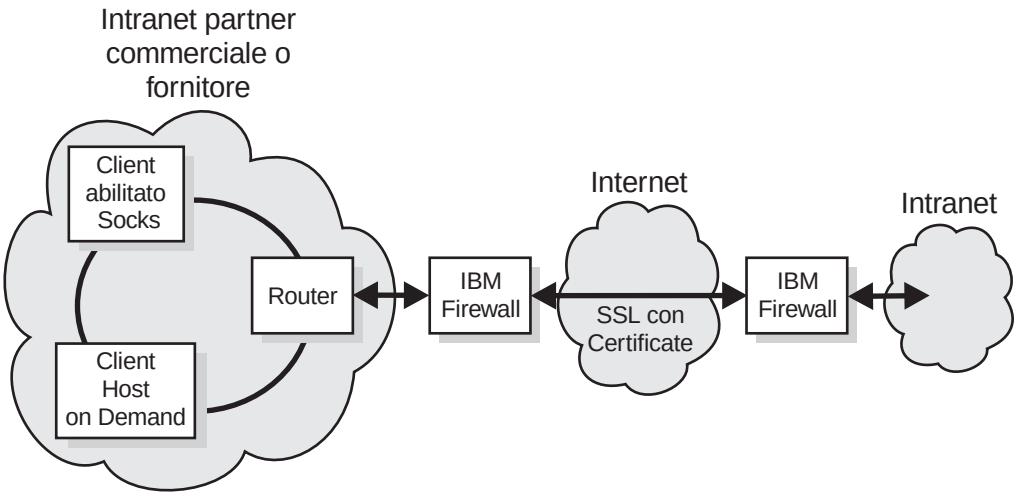


Figura 9. Intranet di un fornitore o di un partner commerciale tipico mediante un protocollo di trasmissione SSL (Secure Sockets Layer)

Sicurezza dell'hardware di Trust Authority

Sebbene in questa sezione non venga descritto dettagliatamente il componente Trust Authority, le seguenti considerazioni si riferiscono a tutti i componenti FirstSecure.

Isolamento dell'area

Configurare il server in un ambiente isolato dedicato all'attività della CA. Se possibile, la stanza dovrebbe disporre di mura rinforzate, di una sola parete portante o porta di ferro, di un tetto solido privo di controsoffittatura. La stanza dovrebbe essere dotata inoltre, di un pavimento rialzato per proteggere dalle scariche in caso di incendio.

Manutenzione dell'area

La stanza dovrebbe essere fornita di una unità elettrica continua per i computer, di lampade, di rilevatori di moto e di sistemi di riscaldamento e ventilazione. Occorre inoltre analizzare la ventilazione della stanza per accertarsi che la temperatura sia sufficiente a contrastare il calore generato dalle apparecchiature.

Controllo degli accessi all'area

E' possibile fornire l'accesso ad un'area fisica in diversi modi, ad esempio, utilizzando delle schede magnetiche oppure predisponendo un sistema di apertura delle porte controllato da una tastierina numerica. Per impedire intrusioni non autorizzate da parte di singoli individui, è necessario installare controlli che richiedano la presentazione di credenziali adeguate da almeno due persone con accesso convalidato.

E' inoltre opportuno controllare la stanza per tenere traccia del numero di accessi e dell'identità di coloro che vi accedono. Per garantire la massima

sicurezza, si consiglia di installare delle telecamere all'interno e all'esterno della porta.

Controllo delle comunicazioni

E' necessario non lasciare alcuna porta aperta sul server Trust Authority. E' necessario configurare il sistema affinché esegua il listen delle richieste solo sulle porte esplicitamente assegnate alle applicazioni Trust Authority attive.

Attenersi alle proprie procedure aziendali e ai propri requisiti per rendere sicuro l'hardware utilizzato nel proprio ambiente e-business.

Capitolo 4. Pianificazione di FirstSecure nella propria rete e-business

I capitoli contenuti in questa sezione collegano i prodotti inclusi in FirstSecure al proprio ambiente e-business. Questi capitoli fanno riferimento alle figure nel Capitolo 3, “Panoramica della rete e-business” a pagina 17. Di ciascun prodotto vengono descritti alcuni dettagli. Per informazioni complete su ciascun prodotto, consultare la documentazione che lo accompagna. Gli scenari illustrati costituiscono solo dei suggerimenti.

In ogni scenario vengono eseguite le medesime operazioni di base:

1. Tutte le parti che compongono la rete devono utilizzare un riferimento temporale comune in modo da rendere l'analisi delle registrazioni, più semplici e accurate.
2. Cominciare dalla propria Intranet per installare e verificare i componenti.
3. Quindi, avviare la creazione delle applicazioni all'interno della zona DMZ protetta.
4. Il traffico di dati tra la propria Intranet e la zona DMZ deve passare attraverso un firewall.
5. Creare le proprie applicazioni Internet esterne e controllarle con i dati di prova.
6. Installare un firewall per proteggere il traffico tra Internet e la propria DMZ.
7. Consentire l'accesso agli utenti.

Pianificazione di un sistema FirstSecure completo

Di seguito viene suggerito l'ordine per la disposizione dei prodotti FirstSecure nella rete. E' molto generico. Consultare Parte 3, “Considerazioni sull'installazione e sull'integrazione” a pagina 53 per i requisiti hardware e software particolareggiati di ciascun prodotto e per le considerazioni di integrazione. Consultare inoltre, le istruzioni e i requisiti di installazione forniti con ciascun prodotto. E' possibile che per alcuni prodotti siano disponibili su Internet informazioni più aggiornate. “Informazioni sul Web” a pagina xii elenca i siti Web con le informazioni FirstSecure. Il manuale Redbook, *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498 contiene molti altri scenari particolareggiati.

1. Pianificare i requisiti di sicurezza necessari.
2. Installare Policy Director per soddisfare i requisiti.

3. Creare e verificare l'applicazione server del proprio cliente. Collocare l'applicazione all'interno della Intranet aziendale, non renderla ancora disponibile su Internet.
4. Installare IBM Firewall per proteggere l'applicazione server del cliente.
5. Aggiungere SurfinGate alla zona DMZ.
6. Nella zona DMZ, aggiungere MIMEsweeper e Norton AntiVirus per proteggere le applicazioni quando le si rende disponibili su Internet. Quando le si rende disponibili per il traffico esterno, è necessario configurarle in modo che facciano riferimento ai propri server.
7. Installare il prodotto Tivoli Cross-Site for Security per individuare eventuali dati non desiderati e respingerli.
8. Nella zona DMZ, aggiungere:
   - Server Web
   - Server cataloghi Web
   - Server inventari Web
   - Applicazioni client del cliente
   - Applicazioni client del cliente sicure
   - Uno o più agenti di Cross-Site for Security

   Provare tutte le applicazioni insieme al firewall prima di renderle disponibili al traffico esterno. Utilizzare lo strumento SecureWay Boundary Server's Network Security Auditor per verificare le regole impostate.
9. Installare un'istanza del IBM SecureWay Firewall per proteggere il software all'interno della zona DMZ. La configurazione predefinita dovrebbe essere “No traffic” in modo che sia possibile provare l'installazione prima di renderla disponibile al pubblico.
10. Installare Trust Authority ed emettere i certificati per gli utenti autorizzati.
11. Rendere disponibile l'applicazione su Internet dopo il completamento di tutte le prove.
12. Eseguire Network Security Auditor fuori dal proprio sistema per verificare le regole prima di fornire l'accesso pubblico.
13. Verificare l'esame delle registrazioni create dai programmi del componente FirstSecure.
14. Continuare a controllare le registrazioni di analisi e aggiungere Cross-Site for Security agent alla rete alla stregua di qualsiasi altra applicazione.

Capitolo 5. Pianificazione di Policy Director nella propria rete

FirstSecure fornisce un punto di controllo basato sulla politica di creazione di ambienti Web eterogenei. In ambienti in cui gli utenti accedono a più server Web back-end mediante i browser, Policy Director fornisce:

- Una registrazione singola per ciascun utente del Web
- Verifica dell'identità
- Verifica dell'autorizzazione degli utenti che richiedono l'accesso alle pagine Web protette

Con questo supporto è possibile autorizzare e proteggere:

- Gli strumenti di scambio TCP/IP, come ad esempio HTML, Telnet e POP3
- Applicazioni di altri produttori, ad esempio, sistemi database
- Strumenti di gestione della rete
- Applicazioni sviluppate in proprio

Con FirstSecure, è possibile ottenere un'autentica per Policy Director utilizzando i seguenti meccanismi:

- Autentica di base con SSL (Secure Sockets Layer)
- Collegamenti basati sui moduli con SSL
- SSL mediante certificati client
- Collegamento Kerberos

FirstSecure controlla quindi l'accesso degli utenti autorizzati a oggetti Web e ai servizi di rete individuali e può limitare gli utenti non autorizzati ad una serie secondaria di queste risorse.

Impiego di Policy Director

Policy Director gestisce la corrispondenza tra utenti, gruppi e risorse. Management Console di Policy Director consente di:

- Definire gli utenti e i gruppi che utilizzeranno le proprie risorse.
- Definire gli oggetti che richiedono protezione. Per oggetti si intendono il Web, le porte TCP, i metodi e le interfacce.

- Definire le modalità di accesso degli utenti alle risorse e le regole che proteggeranno le risorse, ad esempio, la lettura, la modifica, la gestione, l'esecuzione o la cancellazione.

Nella seguente tabella vengono illustrate le configurazioni comuni del componente Policy Director. Determinare la configurazione appropriata alla propria rete. Quindi, selezionare i componenti necessari durante l'installazione.

Per ulteriori informazioni, consultare il manuale *IBM SecureWay Policy Director Up and Running*.

Configurazione di esempio	**Componenti installati**
Un server che sta eseguendo una istanza singola di Management server per un dominio di sicurezza. In questo scenario Management server risiede sul proprio sistema. Management server conserva il database delle autorizzazioni principali per il dominio di sicurezza, replica questo database nel dominio sicuro e conserva le informazioni di ubicazione relative ad altre macchine server Policy Director nel dominio sicuro.	Solo Management server
Un server WebSEAL. Questo scenario rappresenta la soluzione per proteggere uno spazio sul Web. WebSEAL supporta i server back-end, per l'alta disponibilità e la tolleranza degli errori.	Security Manager con WebSEAL
Un server NetSEAL. Questo scenario rappresenta la soluzione per proteggere una rete VPN (Virtual Private Network) e fornire un controllo degli accessi per i servizi di rete di terze parti e per quelli acquisiti.	Security Manager con NetSEAL
Una combinazione di server NetSeal e WebSEAL.	Security Manager con WebSEAL e NetSEAL
Un server che fornisce l'accesso al servizio di autorizzazione Policy Director per le applicazioni di altri fornitori.	Authorization server
Un server che fornisce un ambiente di sviluppo ai programmatori che desiderano creare applicazioni di terze parti che utilizzano le API di autorizzazione.	Authorization server e ADK
Un server che fornisce i servizi combinati di tutte le configurazioni precedenti.	Tutti i componenti

Policy Director è un sistema di sicurezza ampiamente distribuito che può disporre i suoi componenti in una vasta gamma di configurazioni su una o più' macchine. Quanto riportato di seguito, è una panoramica della disposizione di Policy Director nella rete. Le istruzioni di installazione complete si trovano in *IBM SecureWay Policy Director Up and Running*.

1. Installare Policy Director security server.

   E' necessario che almeno un computer nel dominio sicuro contenda Policy Director security server per impostare un dominio sicuro Policy Director. Fare riferimento ai manuali di installazione e di gestione e alle risorse di supporto tecnico per le piattaforme richieste.

   I rimanenti server possono funzionare solo con le installazioni di un client DCE (o NetSEAT sui sistemi Windows NT).

2. Installare il server SecureWay Directory (LDAP).
3. Installare Policy Director.
   - Il server di sicurezza Policy Director deve essere disposto per primo (consultare il passo 1).
   - Tutte le installazioni server di Policy Director richiedono Policy Director di base.
   - E' la *prima* o *l'unica* macchina nel dominio sicuro su cui installare Management server.

     Se questa è una macchina *aggiuntiva* in un dominio sicuro esistente che possiede già Management server, non si deve installare un'altra versione. E' necessario che esista solo una istanza di Management server in ciascun determinato dominio sicuro.
   - WebSEAL, NetSEAL e i componenti del server di autorizzazione di terze parti sono facoltativi.
   - Security Manager agisce con WebSEAL per fornire il componente server HTTP WebSEAL e un controllo degli accessi HTTP accurato e con NetSEAL, per fornire il componente di controllo degli accessi TCP/IP meno accurato NetSeal.
4. Installare la console di gestione.

   La console di gestione richiede che sul sistema operativo siano installati sia un client DCE (o NetSEAT per Windows NT)(consultare il passo 1).
5. Le seguenti dipendenze si applicano alle applicazioni sviluppate con Authorization ADK:
   - E' necessario il pacchetto Policy Director.
   - Installare IVAuthADK sulla macchina su cui risiede l'applicazione.
   - Il sistema operativo su cui viene eseguita l'applicazione deve disporre di un client DCE o di NetSEAT per Windows NT.
   - Il dominio sicuro che esegue un'applicazione, deve avere un server di autorizzazione installato su almeno un computer del dominio sicuro. Un ambiente tipico di sviluppo include il server di autorizzazione sullo stesso sistema operativo di Authorization ADK.

Capitolo 6. Pianificazione di SecureWay Boundary Server nella propria rete

FirstSecure fornisce sicurezza alle applicazioni basate sul Web che si avvantaggiano di standard di sicurezza esistenti come SSL (Secure Sockets Layer), SOCKS e IPSEC.

Se l'ambiente operativo include le connessioni tra due parti della rete con caratteristiche di convalida diverse, il componente SecureWay Boundary Server di FirstSecure è di ausilio nell'indirizzamento delle seguenti richieste:

- Connessioni sicure con Internet, riducendo la possibilità di accessi non autorizzati alla propria rete.
- Infrastrutture extranet a larga scala per la condivisione selettiva dei dati con collaboratori e fornitori esterni.
- Utilizzo di Internet o di altri segmenti di rete relativamente non sicuri come ad esempio VPN (virtual private network), con messaggi non resi disponibili al passaggio nell'infrastruttura di rete non sicura.

FirstSecure SecureWay Boundary Server utilizza tecnologie gateway a livello di circuito, proxy, il filtraggio degli indirizzi di rete e del contenuto. Combinando queste tecnologie, SecureWay Boundary Server abilita le operazioni e-business in modo protetto, sicuro e guidato dalle politiche, controllando le comunicazioni tra le rete con caratteristiche di sicurezza differenti.

SecureWay Boundary Server include:

- IBM SecureWay Firewall, che include ACE/Server
- MIMEsweeper per IBM SecureWay Rilascio 2
- SurfinGate 4.05 per Windows NT
- Miglioramenti alla gestione delle politiche

Fare riferimento alla figura Figura 10 a pagina 36 per una panoramica del flusso di dati in un'installazione SecureWay Boundary Server completa.

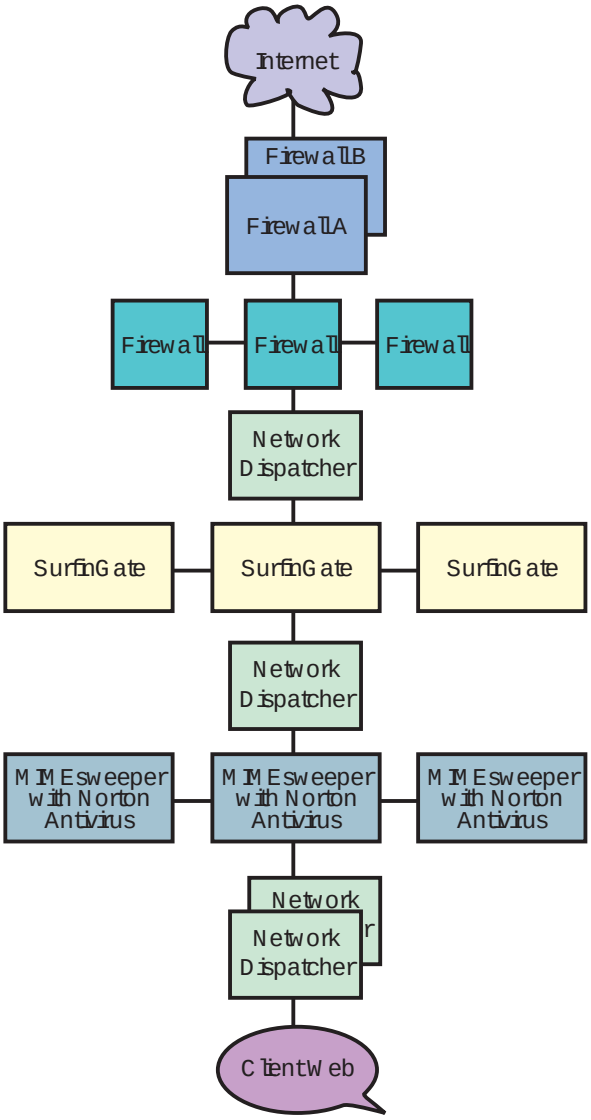


Figura 10. Panoramica del flusso di dati nei prodotti SecureWay Boundary Server

Impiego di IBM SecureWay Firewall

IBM SecureWay Firewall, noto anche come IBM Firewall, controlla le comunicazioni che viaggiano su Internet. La tecnologia firewall protegge i dati della IBM.

Per informazioni sull'installazione, consultare la sezione “Considerazioni sul componente SecureWay Boundary Server” a pagina 62.

Di seguito sono riportati gli obiettivi della creazione di una rete:

- La necessità di collegarsi a Internet prevenendo accessi non autorizzati alla rete, ai dati e alle applicazioni
- L'abuso delle risorse di rete da parte di utenti interni
- La pianificazione di infrastrutture extranet a larga scala per i partner commerciali e per i fornitori nonostante l'alto costo di gestione della configurazione
- Il costo elevato delle linee dedicate alla connessione dei dipartimenti
- Scarsa produttività dovuta da comunicazioni in ritardo, non efficaci o non chiare con i soci o i fornitori.
- L'alto costo di gestione derivante dalla necessità di dover gestire il software in linguaggi non nativi

IBM Firewall risponde a queste preoccupazioni. Permettendo solo il flusso di traffico consentito esplicitamente attraverso il firewall, IBM Firewall protegge la rete dagli estranei. Il software di controllo della vulnerabilità incluso con IBM Firewall può *proteggere* ulteriormente il server su cui IBM Firewall è in esecuzione impedendo agli hacker di entrare o passare nel firewall. Gli indirizzi IP e la configurazione della rete interna sono nascosti dalle reti non convalidate. Tutto il traffico del firewall viene registrato e può essere utilizzato per la creazione di relazioni sull'attività degli utenti.

IBM Firewall e la relativa applicazione di configurazione VPN consentono di disporre e di gestire economicamente infrastrutture VPN ad ampia scala. Studi sulle reti hanno dimostrato che i clienti possono utilizzare VPN per risparmiare sul costo delle soluzioni delle linee in leasing.

Con IBM Firewall, è possibile collegare diversi uffici mediante Internet, inserendo i firewall in ciascun ufficio ed utilizzando un canale basato su IPSEC.

IBM Firewall viene fornito con ACE/Server, un prodotto della Security Dynamics Technologies, Inc. ACE/Server fornisce servizi di autentica centralizzati e potenti per le reti aziendali, in modo che solo gli utenti autorizzati possano accedere ai file di rete, alle applicazioni e alle comunicazioni. Insieme alla tecnologia token SecurID registrata da Security Dynamics Technologies, ACE/Server crea una barriera contro gli accessi non autorizzati. L'autentica si basa su due fattori: agli utenti viene richiesto il *possesso*

di qualcosa (una scheda token SecurID) e la *conoscenza* di qualcosa (un PIN) per ricevere l'autentica.

Impiego di MIMEsweeper

MIMEsweeper è un prodotto della Content Technologies Ltd. che esegue un'analisi in base al contenuto dei dati Internet ed Intranet per individuare tutti i pericoli nascosti e per proteggere gli utenti della rete.

Per informazioni sull'installazione, consultare la sezione “Considerazioni sul componente SecureWay Boundary Server” a pagina 62.

MIMEsweeper contiene due moduli di base, MAILsweeper e WEBsweeper, che proteggono gli utenti in modi diversi. Quando i dati Web e quelli della posta vengono ricevuti da MIMEsweeper, l'applicazione verifica gli indirizzi del mittente e del destinatario e suddivide i file nelle parti che li compongono. MAILsweeper e WEBsweeper analizzano quindi queste parti per proteggere la rete da eventuali pericoli.

FirstSecure include MAILsweeper 4.0 e WEBsweeper 3.2_5. Possono essere installati, configurati e utilizzati separatamente.

MAILsweeper è in grado di:

- Lavorare con programmi di scansione antivirus scelti per verificare che i file suddivisi siano esenti da virus
- Rilevare e bloccare le bombe macro
- Eseguire la scansione di parole chiave nelle operazioni di:
  - Controllo dei messaggi e-mail relativamente all'utilizzo di linguaggio osceno o offensivo
  - Protezione di dati preziosi per evitare che escano dall'azienda
- Bloccare i messaggi e-mail in arrivo non desiderati, decongestionando la rete e riducendo la perdita di produttività del personale
- Bloccare la ricezione o l'invio, per singoli o gruppi, di alcuni file, come ad esempio file AVI o MPEG
- Bloccare o posticipare alcuni file in base alla dimensione, fino a quando la rete non è in grado di poter gestire quel traffico

WEBsweeper è in grado di:

- Impedire l'accesso degli impiegati a siti che non hanno pertinenza con il lavoro
- Impedire la perdita di documenti preziosi o riservati

Inoltre MIMEsweeper contiene una API (application programming interface) che può essere utilizzata per integrare programmi di blocco URL di altri produttori.

MIMEsweeper può essere una grande risorsa per la protezione dell'azienda e degli utenti contro i pericoli di attacchi alla sicurezza provenienti da Internet.

Nota: Sebbene la documentazione di MIMEsweeper fornisca un contatto per l'assistenza ed il supporto Content Technologies, se MIMEsweeper per IBM SecureWay Rilascio 2 viene fornito come parte dell'offerta SecureWay FirstSecure o di quella SecureWay Boundary Server, occorre contattare l'IBM per l'assistenza ed il supporto.

Impiego di SurfinGate

SurfinGate è un prodotto della Finjan Software Ltd., esamina codici mobili, ad esempio il codice JavaScript, le applet Java e i controlli ActiveX per proteggere la rete da danni quali la modifica dei dati, la cancellazione di informazioni e la raccolta illegale di dati. SurfinGate esamina il codice mobile a livello gateway ed identifica il codice pericoloso prima che possa accedere alla rete. Il codice mobile può essere bloccato o consentito in base all'utente o al dipartimento. Inoltre al codice può essere consentito o negato l'accesso alla rete aziendale in base alla funzione prevista del codice. Con SurfinGate, i responsabili possono abilitare il codice mobile e gestire, controllare e aumentare la politica di sicurezza per ActiveX, Java, Javascript, Visual Basic Script, plug-in e cookie.

SurfinGate include i seguenti componenti:

- SurfinGate Server
- SurfinConsole
- SurfinGate database
- Plugin per l'integrazione WTE

SurfinGate Server opera come un server proxy HTTP o come un servizio per il firewall o proxy. SurfinGate Server può essere collocato dopo il firewall aziendale e qualsiasi altro proxy esistente e agisce anche come server HTTP. Questa architettura consente di arrestare ed ispezionare il traffico di codice mobile prima che avvenga l'attacco.

Un responsabile di sistema utilizza SurfinConsole per gestire ed impostare una politica di sicurezza aziendale centrale per il codice mobile. SurfinConsole può controllare più SurfinGate Server sulla rete e può rafforzare le regole per il codice mobile dell'azienda per utenti o gruppi o mediante elenchi personalizzati di codici accettati e non accettati.

SurfinGate database memorizza i dettagli degli ASP (Applet Security Profiles), includendo le informazioni su utenti e gruppi e le relative politiche di sicurezza. Poiché SurfinGate esamina il contenuto di tutti i codici mobili dinamicamente, il database non è necessario per la sicurezza ma è di ausilio per incrementare le prestazioni per le operazioni di grandi entità.

Nota: Sebbene la documentazione di SurfinGate fornisca un contatto per l'assistenza ed il supporto Finjan Technologies, se SurfinGate per Windows NT viene fornito come parte dell'offerta SecureWay FirstSecure o di quella SecureWay Boundary Server, occorre contattare l'IBM per l'assistenza ed il supporto.

Capitolo 7. Pianificazione di Intrusion Immunity nella propria rete

Le tecnologie di sicurezza descritte fino ad ora riguardano la protezione da attacchi alla sicurezza. Un altro aspetto altrettanto importante della sicurezza è la rilevazione dei pericoli. I prodotti per la protezione da intrusioni in FirstSecure forniscono funzioni di rilevazione e funzioni antivirus che consentono all'azienda di rilevare eventuali pericoli.

Il software antivirus fornisce la protezione da tutti i tipi di codice pericolosi, Trojan horse, worm, macro virus, virus dei controlli ActiveX e delle Applet Java. La protezione dai virus è una parte fondamentale di tutte le soluzioni di sicurezza. I prodotti antivirus FirstSecure rispondono ai seguenti requisiti chiave antivirus:

- La copertura di una ampia gamma di client in base alle richieste complete ed efficaci di una protezione antivirus sui client mobili e fissi.
- Servizio abbonamento per le tabelle antivirus. L'aggiornamento delle tabelle dei virus su basi regolari è fondamentale per mantenere una protezione effettiva contro le forme più recenti di codice pericoloso.
- Distribuzione guidata dalle politiche di aggiornamenti antivirus dai server ai client per garantire l'efficacia delle politiche stesse.

Impiego di Tivoli Cross-Site for Security

Tivoli Cross-Site for Security consente di individuare i dati non desiderati basata sulla rete in sistemi vulnerabili. E' possibile collocare gli agenti Tivoli Cross-Site for Security ovunque il proprio dominio di gestione è collegato a Internet. Tivoli Cross-Site for Security controlla le reti per individuare attacchi esterni ed interni. Consente di ottenere i seguenti vantaggi:

- Individuazione delle intrusioni in tempo reale che avverte il responsabile Cross-Site for Security dell'esistenza di potenziali attacchi
- Politica che è possibile configurare che consente di impostare politiche diverse per gli agenti nella propria zona DMZ e quelli presenti sulla Intranet
- Modifica in linea delle politiche relative agli agenti per rispondere rapidamente alle modifiche dell'ambiente
- Integrazione con le applicazioni Tivoli Enterprise che consente di migliorare il sistema di gestione di Tivoli enterprise

Tivoli Cross-Site for Security è in grado di:

- Rilevare le scansioni e le intrusioni
- Controllare il traffico IP
- Controllare i servizi delle porte
- Rilevare le richieste dei file system di rete, dei servizi di montaggio e DNS e rispondere a tali richieste
- Rilevare le richieste di servizio del programma di mappatura delle porte e i dump di risposta
- Individuare le chiamate RStatd
- Rilevare le richieste per nomi file e nomi di corrispondenza specifici
- Rilevare attacchi di tipo SMB sui server di file di un PC
- Rilevare il protocollo dei messaggi di controllo Internet

Cross-Site for Security consente di controllare il traffico di rete e di individuare attacchi e tentativi di intrusione. Controlla in entrambe le DMZ, il traffico che isola Intranet da Internet e sulla rete interna.

I tipi di intrusione che Cross-Site for Security può individuare includono:

- Firma o modello, rilevazione
- Individuazione del flusso
- Attacchi alla rete
- Attacchi alla rete Windows
- Attacchi di procedura remota
- Utilizzo del servizio
- Traffico di rete non autorizzato
- Attività sospette

Cross-Site for Security protegge la rete mediante Cross-Site for Security agent e Cross-Site for Security management server. Quando un agente rileva un attacco critico, invia un evento cifrato a Cross-Site for Security management server che registra immediatamente le informazioni e risponde all'attacco. E' possibile configurare Cross-Site for Security management server per inviare un avviso alla console, un e-mail al responsabile di sistema o inviare un messaggio sul pager di un responsabile.

Come ottenere una chiave di licenza Tivoli Cross-Site for Security

Per abilitare il prodotto Tivoli Cross-Site for Security, è necessario disporre di una chiave di licenza personalizzata.

Per ottenere la chiave di licenza, visitare il sito Web Tivoli Cross-Site ed attenersi alla seguente procedura:

1. Individuare il documento Passport Advantage Proof of Entitlement fornito con i prodotti FirstSecure, inclusi il CD-ROM di Tivoli Cross-Site for Security e il manuale *Tivoli Cross-Site for Security Installation*.
2. Individuare il numero di ordine, un numero costituito da 8 cifre che inizia con 5, il numero (sito) del cliente, un numero costituito da 7 cifre che inizia con 7 sul documento Passport Advantage Proof of Entitlement. L'utente utilizzerà questi numeri per accedere al sito Web di Tivoli Cross-Site per la prima volta.
3. Accedere al sito Web di Tivoli Cross-Site mediante un browser Web su un computer dotato di accesso a Internet. L'URL del sito Web è `www.cross-site.com/support/licensing/`.
4. Inserire il proprio numero di ordine, il numero del cliente e le informazioni sui contatti. E' inoltre necessario fornire il nome di dominio del server su cui verrà installato Tivoli Cross-Site for Security.
5. Attenersi alle istruzioni fornite nella pagina Web.
6. Se si incontrano difficoltà ad accedere al sito Web della chiave di licenza Tivoli Cross-Site , rivolgersi al supporto Tivoli Cross-Site al numero 1–800–2–TIVOLI, interno 9396 o via posta elettronica all'indirizzo licensing@cross-site.com.

Prodotti Tivoli Cross-Site correlati

La famiglia dei prodotti Tivoli Cross-Site include altri componenti che non fanno parte della famiglia FirstSecure:

- Tivoli Cross-Site per Availability controlla e notifica gli accessi degli utenti al sito Web.
- Tivoli Cross-Site per Deployment amplia gli obiettivi della società, consentendo di distribuire e gestire applicazioni e informazioni critiche su Internet.

La documentazione di Tivoli Cross-Site for Security contiene riferimenti a questi prodotti, devono essere acquistati separatamente.

Monitoraggio del traffico con Tivoli Cross-Site for Security

Cross-Site for Security agent controlla le attività di rete. Controlla continuamente i pacchetti presenti sulla rete. Cross-Site for Security agent filtra i pacchetti per individuare elementi relativi ad eventuali attività sospette. Questi elementi possono indicare degli attacchi alla rete.

Cross-Site for Security agent viene eseguito come *daemon* in UNIX e come servizio NT in Windows NT. Cross-Site for Security è configurato per l'avvio automatico

all'avviamento del sistema. Continua ad essere attivo sullo sfondo anche se l'utente non è collegato.

Se viene individuato un potenziale attacco, gli agenti ne determinano la gravità e decidono se notificare la notizia al Management server immediatamente o se registrare il messaggio in un file locale. Le registrazioni vengono caricate periodicamente sul Management server.

L'agente, inoltre, contatta ad intervalli regolari Cross-Site for Security management server per informarlo dello stato di attività dell'agente. Questo tipo di comunicazioni è definito *heartbeat*. L'utente può configurare gli intervalli degli heartbeat.

Quando il server di gestione riceve un heartbeat dall'agente, notifica l'agente di tutte le informazioni di configurazione, delle nuove firme e delle pianificazioni di scaricamento. L'agente automaticamente scarica e installa questi aggiornamenti.

Tivoli Cross-Site for Security nella propria rete

Cross-Site for Security può essere configurato per soddisfare i requisiti della propria azienda. Le decisioni principali sono:

- Dove installare Cross-Site for Security management server
- Quanti agenti di Cross-Site for Security sono necessari
- Dove installare gli agenti di Cross-Site for Security

Queste considerazioni, oltre a quelle relative alle dimensioni, alla topologia, al traffico e alla larghezza di banda della rete sono fondamentali per determinare il numero di Management server e di agenti. Per informazioni sull'installazione di Tivoli Cross-Site for Security, consultare la sezione “Requisiti hardware e software di Intrusion Immunity” a pagina 67.

Nota: Sebbene la documentazione di Tivoli Cross-Site for Security contenga informazioni sull'assistenza e sul supporto, se Tivoli Cross-Site for Security viene fornito come parte dell'offerta SecureWay FirstSecure, occorre contattare l'IBM per l'assistenza ed il supporto.

Impiego di Norton AntiVirus

Norton AntiVirus, un prodotto della Symantec Corporation, è uno dei prodotti software antivirus più diffuso nel mondo. Norton AntiVirus è in grado di:

- Isolare i file infetti
- Proteggere da virus e da controlli ActiveX e applet Java pericolosi

- Proteggere dai virus che possono essere introdotti mediante la posta elettronica, gli scaricamenti di programmi da Internet, i minidischi, i CD dei software o reti infette.

Norton AntiVirus può essere eseguito costantemente in background per garantire la sicurezza del proprio computer. I ricercatori della Symantec continuano ad aggiungere nuovi virus che Norton AntiVirus può individuare. E' possibile utilizzare la funzione LiveUpdate per richiamare automaticamente le nuove definizioni antivirus da Symantec una volta a settimana.

La funzione di isolamento di Norton AntiVirus 5.0 isola i file infetti o sospetti in un'ubicazione sicura sul computer, separandoli dagli altri file per evitare l'espansione del virus.

La procedura guidata Scan and Deliver consente di inviare i file sospetti alla Symantec per un esame. Il centro SARC (Symantec AntiVirus Research Center) fornirà informazioni utili per risolvere il problema.

Il programma di scansione Norton AntiVirus, denominato *Bloodhound* viene eseguito sullo sfondo per controllare e catalogare il comportamento di applicazioni che possono essere infettate dai nuovi virus. Se un'applicazione si comporta come un virus e tenta di infettare altri programmi, Bloodhound può arrestare il programma, impedendo l'infezione di altri file fino a quando non si ricevono i nuovi aggiornamenti per i virus.

I prodotti Norton AntiVirus Solution Rilascio 3.04 forniti con FirstSecure sono:

- Soluzioni desktop:
  - Norton AntiVirus 4.08 per DOS
  - Norton AntiVirus 4.08 per Windows 3.51
  - Norton AntiVirus 5.02 per Windows 95/98
  - Norton AntiVirus 4.08 per Windows NT 3.51
  - Norton AntiVirus 5.02 per Windows NT 4.0
  - Norton AntiVirus 5.03 per Macintosh
  - Norton AntiVirus 5.02 per OS/2
- Soluzioni server:
  - Norton AntiVirus 4.08 per Windows NT 3.51
  - Norton AntiVirus 5.02 per Windows NT 4.0
  - Norton AntiVirus 4.04 per NetWare
  - Norton AntiVirus 2.0 per Lotus Notes™ e OS/2
  - Norton AntiVirus 1.52 per Microsoft Exchange
- Soluzioni gateway:
  - Norton AntiVirus 1.02A per Internet E-mail Gateway per NT
  - Norton AntiVirus 1.04 per Firewalls
- Gestione:
  - Norton System Center 3.1
  - Norton AntiVirus 5.03 per Macintosh Administrator
  - Norton AntiVirus Plus 5.0 per Tivoli Enterprise
  - Norton AntiVirus Plus 5.0 per Tivoli IT Director

– Altri strumenti di gestione, incluso Norton AntiVirus Network Manager (NAV32/NAVNETW) v3.01

Ulteriori informazioni su Norton AntiVirus sono contenute nel file contents.txt nella directory principale del CD di Norton AntiVirus.

Nota: Sebbene la documentazione Norton AntiVirus fornisca un contatto con la Symantec per l'assistenza ed il supporto, se Norton AntiVirus Solution Rilascio 3.04 viene fornito come parte dell'offerta SecureWay FirstSecure, occorre contattare l'IBM per l'assistenza ed il supporto.

Per informazioni dettagliate sulla procedura di installazione, consultare la documentazione fornita con i singoli prodotti e i requisiti hardware e software nel capitolo Capitolo 13, “Intrusion Immunity - Requisiti e considerazioni sull'installazione” a pagina 67.

Capitolo 8. Pianificazione di Public Key Infrastructure nella propria rete

Il componente Trust Authority di Public Key Infrastructure fornisce le applicazioni Internet gli strumenti per eseguire l'autentica degli utenti e per garantire la sicurezza delle comunicazioni. Basata sugli standard PKI (public key infrastructure) per la cifratura e l'interoperabilità, un sistema Trust Authority fornisce l'infrastruttura necessaria per emettere, pubblicare e gestire i certificati digitali. Comprende:

- Il supporto per piattaforme IBM AIX e Microsoft Windows NT server.
- Una RA (Registration Authority) che gestisce le attività di gestione che sono alla base della registrazione degli utenti. Questa gestione, che può essere realizzata mediante processi automatici o decisioni da parte degli utenti, include i seguenti tipi di attività:
  - Conferma dell'identità dell'utente
  - Approvazione o rifiuto delle richieste di rilascio, rinnovo o revoca dei certificati
  - Verifica del possesso da parte dell'utente della chiave privata associata alla chiave pubblica in un certificato
  - Utilizzo delle regole in un determinato processo aziendale o nel profilo di un certificato per emettere determinati tipi di certificato per determinati tipi di utente.

  La RA, inoltre, pubblica le informazioni sui certificati in una directory di chiavi pubbliche integrata, IBM SecureWay LDAP Directory.
- Una CA (Certificate Authority) convalidata. La CA esegue le seguenti attività:
  - Emette i certificati digitali e crea le coppie di chiavi digitali che consentono l'autentica dei certificati
  - Segue l'intero corso di vita dei certificati, dall'iscrizione iniziale al rinnovo e alla revoca
  - LA RA aggiorna la Directory subito dopo la revoca di un certificato
  - Può avvalersi di un hardware cifrato, ad esempio IBM SecureWay 4758 PCI Cryptographic Coprocessor e schede intelligenti per estendere le funzioni di protezione delle chiavi
- Credential Central, un'interfaccia di iscrizione basata sul Web che facilita il rilascio di certificati per browser, server e per alcuni dispositivi, ad esempio, le schede intelligenti. I responsabili possono inoltre utilizzare questi moduli di iscrizione per registrare in anticipo gli utenti finali per un certificato PKIX.
- Trust Authority Client, un'interfaccia Windows indipendente che consente agli utenti di ottenere, rinnovare e revocare i certificati PKIX senza utilizzare un browser Web.

- RA Desktop, un'interfaccia di gestione basata sul Web che consente ai responsabili di approvare o respingere le richieste di rilascio, rinnovo o revoca dei certificati.
- Un sistema secondario di analisi che utilizza i MAC (message authentication codes) per assicurarsi dell'autenticazione degli eventi che riceve da Trust Authority RA e CA. Una opzione configurabile consente ai record di analisi di essere protetti nell'integrità quando vengono registrati.
- Esistono diverse interfacce di gestione per la configurazione del sistema, per la modifica delle password di protezione, la certificazione incrociata della CA, la registrazioni di analisi dei controlli di integrità e per l'avvio e l'arresto protetto dei componenti di sistema.
- Un'API (application programming interface) che consente ai programmatori di scrivere applicazioni personalizzate PKI.
- Supporto run-time integrato per IBM DB2 Universal Database. IBM SecureWay Directory, le RA, le CA e i componenti di Audit dispongono di database separati.

Impiego di Trust Authority

Per informazioni dettagliate sulla pianificazione e sull'installazione, consultare il manuale *IBM SecureWay Trust Authority Up and Running*. Questo manuale contiene gli scenari e le procedure per l'installazione sui server Windows NT e AIX.

Capitolo 9. Pianificazione di SecureWay Toolbox nella propria azienda

Pianificare l'installazione di FirstSecure Toolbox in un ambiente di sviluppo, non nella propria rete. Verificare le proprie applicazioni all'interno dell'ambiente di sviluppo prima di renderle disponibili ad altri utenti.

Servizi per la gestione delle autorizzazioni

I servizi per la gestione delle autorizzazioni consentono di verificare quali utenti sono autorizzati ad accedere al proprio sito Web. L'autentica si basa sulle password o sulle chiavi pubbliche. Queste misure proteggono l'integrità e la riservatezza dei dati nel proprio sito. I servizi per la gestione delle autorizzazioni creano gli ACL (access control lists) che definiscono gli utenti che possono accedere agli oggetti presenti nel sito e le modalità di accesso. Consentono inoltre di definire gli oggetti protetti e di creare delle password per registrazioni singole. Tutti questi strumenti per la sicurezza sono centralizzati per facilitare la gestione delle politiche di sicurezza. Authorization services sono supportati dalle API di autorizzazione di IBM SecureWay Policy Director.

Servizi CA (Certificate authority)

I servizi CA (Certificate authority) sono supportati da X.509 Public Key Infrastructure for Multiplatforms e IBM KeyWorks Toolkit.

Garantiscono la sicurezza nella gestione dei certificati digitali. Questi servizi includono le API relative all'intero ciclo di vita dei certificati: rilascio, rinnovo e revoca. Curano inoltre la pubblicazione di elenchi di revoca dei certificati. Le API utilizzano la cifratura della chiave pubblica e la tecnologia delle schede intelligenti per autenticare gli utenti dei certificati.

X.509 Public Key Infrastructure for Multiplatforms, noto anche come PKIX, viene fornito mediante le API di PKIX. Queste API consentono la creazione, la gestione, la memorizzazione, la distribuzione e la revoca dei certificati mediante i componenti EE (end entity), CA (certificate authority) e RA (registration authority). Le API sono compatibili con IBM SecureWay Trust Authority e sono basate su IBMKeyWorks.

Per informazioni sulle API di PKIX, consultare il manuale *IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference*. Per ulteriori informazioni su IBM KeyWorks, consultare il capitolo Capitolo 16, “Documentazione fornita con FirstSecure” a pagina 87 per un elenco della documentazione fornita con Toolbox.

Servizi di Directory

I servizi di Directory sono supportati da IBM SecureWay Directory Client.

I servizi di Directory utilizzano Lightweight Directory Access Protocol (LDAP) per organizzare, controllare e accedere alle directory. Questi servizi si basano su un modello client/server che fornisce l'accesso client ad un server LDAP. I servizi di Directory costituiscono uno strumento per la conservazione delle informazioni delle directory in una collocazione centrale per la memorizzazione, gli aggiornamenti, il richiamo e lo scambio. I servizi di Directory utilizzano SSL (Secure Sockets Layer) per cifrare le informazioni.

Per ulteriori informazioni sui servizi di directory, consultare il Capitolo 16, “Documentazione fornita con FirstSecure” a pagina 87 per un elenco completo della documentazione di IBM SecureWay Directory Client fornita con Toolbox.

Servizi di cifratura e gestione della sicurezza KeyWorks

I servizi di cifratura e gestione della sicurezza sono supportati da IBM KeyWorks Toolkit, noto anche come KeyWorks.

I servizi di cifratura e gestione della sicurezza KeyWorks consentono di cifrare e di annullare la cifratura delle informazioni per verificare chi ha accesso alle informazioni. Questi servizi creano e verificano le firme digitali per autenticare le identità di individui e computer nelle reti. Un sistema di recupero chiavi che abilita il recupero delle informazioni cifrate, senza distribuire le chiavi è integrato con IBM Key Recovery Service Provider.

KeyWorks è un toolkit di servizi per la cifratura e la sicurezza. E' costituito da una serie di servizi su vari livelli e dalle relative interfacce di programmazione che forniscono una serie integrata di informazioni e di funzioni per la sicurezza delle comunicazioni. Ciascun livello si basa sui servizi principali del livello sottostante. I livelli inferiori sono

caratterizzati dai componenti fondamentali, ad esempio gli algoritmi di cifratura, i numeri casuali e le informazioni per l'identificazione univoca. I livelli superiori si caratterizzano per i certificati digitali, i meccanismi di gestione delle chiavi e di recupero e i protocolli per garantire la sicurezza delle transazioni.

KeyWorks è abilitato per NLS (National Language Support), pertanto, non è dipendente da lingua, cultura e code page specifiche.

Per ulteriori informazioni sulle API KeyWorksC, consultare il Capitolo 16, “Documentazione fornita con FirstSecure” a pagina 87 per un elenco della documentazione KeyWorks fornita con Toolbox.

Servizi di protocollo Secure Sockets Layer

I servizi di protocollo Secure Sockets Layer sono supportati da IBMSecure Sockets Layer (SSL) Toolkit.

I servizi di protocollo SSL consentono di stabilire quali utenti avranno accesso ai propri dati. Questi servizi eseguono la cifratura dei dati utilizzando chiavi pubbliche e private per diversi scopi, ad esempio per autenticare gli utenti, per impedire l'accesso da parte di client non autorizzati e la falsificazione dei dati. In tal modo, è possibile controllare gli utenti per i quali vengono rilasciati i certificati e coloro ai quali viene fornito l'accesso ai propri dati. La tecnologia SSL è inserita in diverse altre API per la cifratura dei dati e la creazione di password.

Parte 3. Considerazioni sull'installazione e sull'integrazione

In questa sezione vengono illustrate le modalità di interazione dei componenti. Vengono elencati i requisiti hardware e software per ciascun prodotto, le applicazioni richieste o i prodotti del database.

Capitolo 10. Pianificazione dell'installazione di FirstSecure

Prima di installare i prodotti del componente FirstSecure, leggere le seguenti sezioni per verificare i requisiti software e hardware. Informazioni aggiornate su FirstSecure sono disponibili all'indirizzo www.ibm.com/software/security/firstsecure . Prima di avviare l'installazione dei prodotti, consultare il sito Web per verificare gli ultimi aggiornamenti.

Istruzioni dettagliate per l'installazione e la configurazione dei prodotti del componente FirstSecure sono fornite nelle pubblicazioni relative ai prodotti di ciascun componente.

Requisiti generali di sistema

In questa sezione vengono illustrati i requisiti generali di sistema per i prodotti FirstSecure. Per informazioni sui requisiti hardware e software specifici di ciascun prodotto del componente, fare riferimento al prodotto del componente richiesto.

Per installare i componenti di FirstSecure, è necessario disporre di un hardware su cui è possibile installare uno dei seguenti sistemi operativi server:

- Microsoft Windows NT Versione 4 con Service Pack 5.
- AIX Versione 4.3.1 o versione successiva.
- Sun Solaris Versione 2.6 o versione successiva.

  Nota: In ambiente Solaris, Toolbox richiede Sun Solaris Versione 2.6 con FixPak del mese di maggio 1999.

Ognuno dei prodotti del componente FirstSecure viene eseguito su almeno uno dei sistemi operativi indicati. La sezione di ciascun prodotto del componente illustra i sistemi operativi supportati ed altri software prerequisiti. Ciascun sistema operativo dovrà disporre di server, di console di gestione e di client. Nelle seguenti sezioni viene fornita una panoramica dei requisiti.

Requisiti del sistema operativo per server e client

Per informazioni sui requisiti del sistema operativo per i prodotti SecureWay consultare la tabella Tabella 1 a pagina 56.

Tabella 1. Requisiti del sistema operativo per server e client		
Sistema operativo	**Livello server minimo**	**Livello client minimo**
Windows NT	Versione 4.0, Service Pack 5	Versione 4.0, Service Pack 5
IBM AIX	Versione 4.3.1	Versione 4.3.1
Sun Solaris	Versione 2.6	Versione 2.6
Windows 95	Non disponibile	Tutte le versioni
Windows 98	Non disponibile	Tutte le versioni
Windows 3.1 (solo Norton AntiVirus)	Non disponibile	Tutte le versioni
IBM OS/2 (solo Norton AntiVirus)	Non disponibile	Versione 4.0, FixPak 6 o successivo

Requisiti ed informazioni relativi ai prodotti del componente

Le sezioni seguenti illustrano i requisisti hardware e software dei prodotti del componente FirstSecure. Vengono illustrati i requisiti hardware e software e le procedure di installazione di ciascuno di essi. Viene inoltre fornita una panoramica della configurazione e dell'installazione di ciascun prodotto e dell'integrazione dei componenti.

- Capitolo 11, “Policy Director - Requisiti e considerazioni sull'installazione” a pagina 57
- Capitolo 12, “SecureWay Boundary Server - Requisiti e considerazioni sull'installazione” a pagina 59
- Capitolo 13, “Intrusion Immunity - Requisiti e considerazioni sull'installazione” a pagina 67
- Capitolo 14, “Public Key Infrastructure - Requisiti e considerazioni sull'installazione” a pagina 75
- Capitolo 15, “Toolbox - Requisiti e considerazioni sull'installazione” a pagina 81

Capitolo 11. Policy Director - Requisiti e considerazioni sull'installazione

Questo capitolo contiene informazioni sui requisiti hardware e software di Policy Director. Contiene inoltre considerazioni sull'installazione in relazione all'integrazione con altri prodotti FirstSecure.

Requisiti hardware e software di Policy Director

La Tabella 2 elenca i requisiti hardware di Policy Director.

Tabella 2. Requisiti hardware di Policy Director

Piattaforma	Spazio su disco minimo	Memoria minima
Windows NT server: Intel o compatibile con Intel 80486 133 MHZ o successivo	16 MB	64 MB
AIX server: hardware eseguito in AIX 4.3.1	16 MB	64 MB
Solaris server: hardware eseguito in Solaris 2.6	16 MB	64 MB

Requisiti software per i componenti di Policy Director:

Server di Policy Director

- Windows NT Server Versione 4.0, Service Pack 5
- AIX Versione 4.3.1
- Sun Solaris, Versione 2.6

Client NetSEAT

- Windows NT Server Versione 4.0, Service Pack 5
- Windows 95
- Windows 98

Management console

- Windows NT Workstation
- Windows NT Server Client
- AIX Versione 4.3.1 Client
- Sun Solaris, Versione 2.6 Client

Policy Director richiede altri software forniti insieme al pacchetto. Per installare il software richiesto per Policy Director, attenersi alle informazioni contenute in *IBM SecureWay Policy Director Up and Running*.

Considerazioni sull'installazione di Policy Director

La pagina Web www.ibm.com/software/security/policy contiene gli aggiornamenti ai prerequisiti software di Policy Director.

Integrazione di Policy Director e Trust Authority

La IBM SecureWay Trust Authority provvede all'autentica, accertando l'identità degli utenti. La Trust Authority fornisce i certificati agli utenti in base alle informazioni contenute in IBM SecureWay Directory, nota anche come Lightweight Directory Access Protocol o LDAP.

Policy Director utilizza i certificati e concede le autorizzazioni, verificando che gli utenti possano accedere solo alle risorse per le quali sono autorizzati. Policy Director memorizza le informazioni in IBM SecureWay Directory.

La propria rete e-business può disporre di una singola definizione utente con tutte le autorizzazioni di Policy Director e tutte le informazioni di Trust Authority. Inoltre, memorizzando le informazioni di SecureWay Boundary Server in IBM SecureWay Directory, Policy Director le gestirà in luogo dell'utente.

Capitolo 12. SecureWay Boundary Server - Requisiti e considerazioni sull'installazione

Questo capitolo contiene informazioni sui requisiti hardware e software di SecureWay Boundary Server. Contiene inoltre considerazioni sull'installazione in relazione all'integrazione con altri prodotti SecureWay Boundary Server.

Requisiti hardware e software di SecureWay Boundary Server

I requisiti hardware per i prodotti del componente SecureWay Boundary Server sono illustrati nella Tabella 3 a pagina 60 e nella Tabella 4 a pagina 61.

Tabella 3. Requisiti hardware per i prodotti del componente SecureWay Boundary Server

Componente SecureWay Boundary Server	**Tipo di macchina**	**Spazio su disco**	**Memoria**	**Altro**
IBM SecureWay Firewall[1]	NT: Pentium 133 MHz o superiore AIX: RS/6000 con supporto AIX 4.3.2	NT: 24 MB[2] AIX: 307 MB	NT: 64 MB AIX: 64 MB	2 schede interfaccia rete
ACE/Server	NT: Pentium a 166 MHz o superiore (solo processore singolo) AIX: Macchina con supporto AIX 4.2	Software server principale: 50 MB Server di backup: 22 MB Database utente iniziale: 4 MB Installazione: 240 MB	Minimo: 32 MB	I requisiti di memoria effettivi sono basati sul numero di utenti
SurfinGate				
Server	Pentium a 233 MHz o superiore	20 MB	Minimo: 128 MB Consigliati: 256 MB	
Console	Pentium a 233 MHz o superiore	15 MB	Minimo: 32 MB Consigliati: 64 MB	
MIMEsweeper per IBM SecureWay Rilascio 2				
MAILsweeper	Pentium a 200 MHz o superiore	1 GB	64 MB	1 scheda di interfaccia rete
WEBsweeper	Pentium a 400 MHz o superiore	1 GB	128 MB + 1 MB per ogni connessione Web contemporanea	1 scheda di interfaccia rete

Note:

1. Per ulteriori informazioni, consultare la documentazione fornita con IBM Firewall.
2. Inoltre, sono richiesti 13 MB di spazio su disco per il browser Netscape.

Tabella 4. Requisiti software per i prodotti del componente SecureWay Boundary Server

Componente SecureWay Boundary Server	**Piattaforme Microsoft Windows**		**AIX**	**Solaris**
	Client	**Server**	**Server**	**Server**
IBM SecureWay Firewall	Windows 95, client IPSec	Windows NT Server Versione 4.0, Service Pack 5[1]	AIX 4.3.2	Non disponibile
ACE/Server	Windows NT Workstation 4.0, Service Pack 2 o successivo	Windows NT Server Versione 4.0, Service Pack 5 o successivo	AIX 4.2	Solaris 2.5.1
SurfinGate 4.05				
Server	Non disponibile	Windows NT 4.0[2]	Non disponibile	Non disponibile
Console	Windows NT 4.0 o successivo [2] Windows 95, Windows 98	Non disponibile	Non disponibile	Non disponibile
MIMEsweeper per IBM SecureWay Rilascio 2				
MAILsweeper	Non disponibile	Windows NT 4.0[3]	Non disponibile	Non disponibile
WEBsweeper	Windows NT Workstation 4.0, Service Pack 3 o successivo	Windows NT 4.0[4]	Non disponibile	Non disponibile

Note:

1. Per prendere visione delle correzioni richieste, consultare la documentazione fornita con IBM Firewall per Windows NT.
2. Inoltre:
   - E' richiesto il client di rete Windows per Microsoft Windows.
   - Windows NT Workstation non è supportato.
3. Inoltre:
   - NT 3.5.1 e Windows NT Workstation non sono supportati.
   - E' richiesto uno dei seguenti ambienti:
     - Microsoft Exchange
     - SMTP
     - cc:Mail
     - Groupwise
     - Lotus Notes
4. Consultare la sezione “Considerazioni su MIMEsweeper” a pagina 65 per informazioni su MIMEsweeper.

Considerazioni sul componente SecureWay Boundary Server

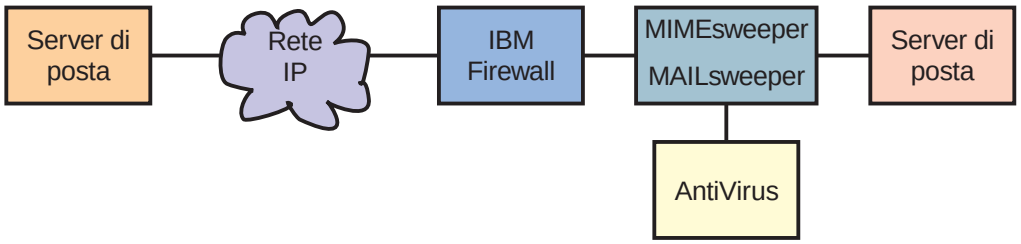
Le seguenti sezioni contengono considerazioni sull'installazione e sulla configurazione dei prodotti del componente SecureWay Boundary Server.

Considerazioni su IBM Firewall

Nelle considerazioni su IBM Firewall viene indicato dove installare questo componente in relazione agli altri prodotti SecureWay Boundary Server.

Configurazioni di esempio

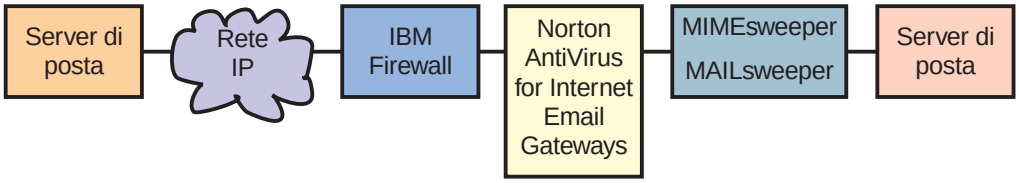
IBM Firewall e MAILsweeper - Configurazione di esempio: Durante l'installazione di IBM Firewall e di MIMEsweeper, è possibile utilizzare la configurazione illustrata in questa sezione.



- MAILsweeper fa parte di MIMEsweeper che controlla il contenuto dei messaggi di posta. MAILsweeper possiede una funzione per abilitare i controlli antivirus.
- MAILsweeper si posiziona tra IBM Firewall ed i server SMPT protetti.
- IBM Firewall fa riferimento a MAILsweeper come l'host della posta a cui i messaggi vanno inoltrati.
  - IBM Firewall richiede che le regole della posta predefinite siano impostate per consentire il flusso del traffico della posta.
- I server SMTP devono inoltre indicare MAILsweeper come l'host della posta cui inoltrare i messaggi.
- MAILsweeper controlla il contenuto dei messaggi inoltrati in entrambe le direzioni.

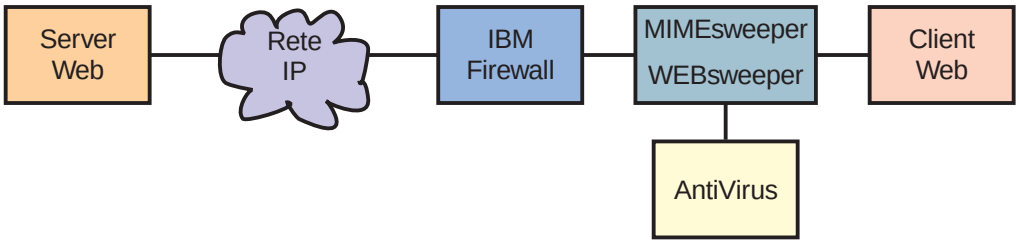
IBM Firewall, Norton AntiVirus per Internet Email Gateway, e MIMEsweeper - configurazione di esempio: Se si installa IBM Firewall, Norton AntiVirus per Internet Email Gateway e MIMEsweeper, è possibile utilizzare la configurazione illustrata in

questa sezione. Lo scenario descritto, associa IBM Firewall, Norton AntiVirus per Internet Email Gateway e MAILsweeper in una catena, per controllare il contenuto della posta, eseguendone anche un controllo antivirus, così come illustrato nel diagramma riportato di seguito.



- Il firewall si riferisce a Norton AntiVirus per Internet Email Gateway come il suo server di posta protetta. Occorre impostare le regole corrette di firewall per consentire questo specifico traffico.
- Norton AntiVirus per Internet Email Gateway si riferisce a MAILsweeper come il programma per l'inoltro di posta protetta e a firewall per la posta in uscita.
- MAILsweeper riceve e controlla la posta inoltrata. Quindi, invia la posta al server corretto in base alle proprie tabelle di instradamento o alle ricerche dei record MX. Se MAILsweeper e Norton AntiVirus per Internet Email Gateway si trovano sulla stessa macchina, occorre modificare la porta di ricezione per MAILsweeper per evitare conflitti con Norton AntiVirus per Internet Email Gateway.

IBM Firewall e WEBsweeper - configurazione di esempio: Se si installa IBM Firewall e MIMEsweeper, è possibile utilizzare la configurazione illustrata in questa sezione.



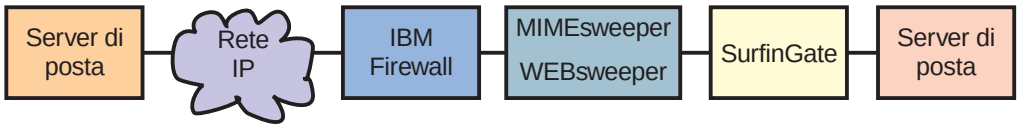
- WEBsweeper fa parte di MIMEsweeper che controlla il traffico Web. WEBsweeper possiede una funzione per abilitare i controlli antivirus.
- WEBsweeper agisce come proxy intermediario. I client specificano WEBsweeper come relativo proxy. WEBsweeper viene quindi impostato per inoltrare il traffico al proxy firewall.
- Le regole devono essere impostate sul firewall per consentire il traffico proxy.
- Le richieste proxy possono provenire solo da una rete protetta che si trova dietro un firewall.
- WEBsweeper non gestisce HTTPS. Per utilizzare HTTPS occorre ignorare WEBsweeper in modo da evitare problemi con il firewall e per assicurarsi che tutto

il traffico Web sia controllato. Specificare direttamente il proxy firewall. Il traffico Web è ancora protetto, ma non viene controllato da WEBsweeper.

IBM Firewall e SurfinGate - configurazione di esempio: Se si installa IBM Firewall e SurfinGate, è possibile utilizzare la configurazione illustrata in questa sezione.

- SurfinGate controlla il traffico Web verificando la presenza dei controlli ActiveX e di altre voci.
- SurfinGate agisce come proxy Web intermediario. I client specificano SurfinGate come relativo proxy per HTTP, FTP e HTTPS. SurfinGate inoltra quindi la richiesta al proxy IBM Firewall.
- Le regole devono essere impostate sul firewall per consentire il traffico proxy.
- Le richieste proxy possono provenire solo da una rete protetta che si trova dietro un firewall.

IBM Firewall, MIMEsweeper, e SurfinGate - configurazione di esempio: Se si installa IBM Firewall, MIMEsweeper e SurfinGate, è possibile utilizzare la configurazione illustrata in questa sezione.



- SurfinGate controlla il traffico Web verificando la presenza dei controlli ActiveX e di altre voci. Utilizza diversi controlli rispetto al componente WEBsweeper di MIMEsweeper.
- SurfinGate e WEBsweeper agiscono come proxy Web intermediari. I client specificano SurfinGate come relativo proxy per HTTP e FTP. SurfinGate inoltra quindi la richiesta a WEBsweeper. WEBsweeper inoltra la richiesta al proxy IBM Firewall.
- Le regole devono essere impostate sul firewall per consentire il traffico proxy. Queste regole sono definite nella pubblicazione *IBM eNetwork Firewall versione 3.3 for Windows NT User's Guide*.
- Le richieste proxy possono provenire solo da una rete protetta che si trova dietro un firewall.
- WEBsweeper non gestisce HTTPS. Per evitare problemi con il firewall e per assicurarsi che tutto il traffico Web sia controllato, durante l'utilizzo di HTTPS occorre ignorare WEBsweeper. Specificare direttamente il proxy firewall. Il traffico Web è ancora protetto, ma non viene controllato da WEBsweeper.

Considerazioni su MIMEsweeper

Viene illustrato di seguito un sistema WEBsweeper tipico:

- Intel Pentium a 400 MHz o superiore
- 1 GB di spazio su disco e 128 MB di RAM
- Windows NT Server o Workstation Versione 4.0 Service Pack 3 o successivo
- Protocollo TCP/IP, inclusi un nome host e di dominio
- Strumenti Antivirus

Viene illustrato di seguito un tipico ambiente WEBsweeper ad elevato volume composto da un numero massimo di 500 utenti contemporanei:

- Due processori Intel Pentium II a 450 MHz o superiore
- 3 GB di spazio su disco e 256 MB di RAM
- Windows NT Server o Workstation Versione 4.0 Service Pack 3 o successivo
- Protocollo TCP/IP, inclusi un nome host e di dominio
- Strumenti Antivirus

Se l'ambiente in uso supporta più di 500 utenti concorrenti, si consiglia di utilizzare più server WEBsweeper.

Capitolo 13. Intrusion Immunity - Requisiti e considerazioni sull'installazione

In questo capitolo vengono illustrati i requisiti hardware e software per i componenti di Intrusion Immunity, Tivoli Cross-Site for Security e Norton AntiVirus.

Requisiti hardware e software di Intrusion Immunity

In questa sezione viene illustrata la documentazione relativa all'installazione e alla configurazione dei prodotti del componente Intrusion Immunity.

I requisiti hardware e software di Tivoli Cross-Site for Security sono illustrati nella Tabella 5 a pagina 68, nella Tabella 6 a pagina 68 e nella Tabella 7 a pagina 69. I requisiti hardware e software per i prodotti del componente Norton AntiVirus sono illustrati nella Tabella 8 a pagina 69 e nella Tabella 9 a pagina 70.

Tabella 5. Requisiti hardware e software per i server Tivoli Cross-Site for Security	
Requisiti server	
Sistema operativo	• AIX 4.3.2 • Windows NT Versione 4.0, Service Pack 5 • Solaris 2.5.1 o 2.6
Java	JDK 1.1.6 revisione 04 o successiva
Server Web	Netscape Enterprise Server 3.51
Database	• IBM DB2 Rilascio 5.2 • Oracle 7.3.4 (o 8.0.4 consigliato) • Microsoft SQL Server
Spazio su disco	• Windows NT 290 MB • AIX 180 MB • Solaris 180 MB
Memoria	256 MB
Spazio di swap	300 MB (consigliati: 400 MB)
Note: 1. Netscape Enterprise Server 3.51 e 3.6 non sono supportati. 2. Prendere visione dei requisiti Patch per Solaris nella documentazione relativa all'installazione di Tivoli Cross-Site for Security.	

Tabella 6. Requisiti hardware e software per Management Console di Tivoli Cross-Site for Security	
Requisiti di Management Console	
Sistemi operativi	• Windows 95 • Windows 98 • Windows NT Versione 4.0, Service Pack 5 (166 MHz o superiore) • Solaris 2.5.1 o 2.6 eseguito in Sun SPARC
Spazio su disco	25 MB per tutte le piattaforme
Memoria	• Windows NT 40 MB • AIX 64 MB • Solaris 40 MB

Tabella 7. Requisiti hardware e software per gli agenti di Tivoli Cross-Site for Security

Requisiti per gli agenti	
Sistemi operativi	• Windows NT Versione 4.0, Service Pack 5 o successivo • AIX 4.3.2 • Solaris 2.5.1 o 2.6 eseguito in Sun SPARC
Java	JDK 1.1.6 revisione 04 o successiva in Solaris (richiesto solo per UNIX)
Spazio su disco	• 15 MB in Windows NT • 10 MB in AIX • 10 MB in Solaris
Memoria	• 32 MB in Windows NT • 32 MB in AIX • 20 MB in Solaris

Note:

1. Netscape Enterprise Server 3.51 e 3.6 non sono supportati.
2. Prendere visione dei requisiti Patch per Solaris nella documentazione relativa all'installazione di Tivoli Cross-Site for Security.

La Tabella 8 elenca i requisiti hardware per Norton AntiVirus.

Tabella 8. Requisiti hardware per Norton AntiVirus.

Componente Intrusion Immunity	**Tipo di macchina**	**Spazio su disco**	**Memoria**	**Altro**
Norton AntiVirus	CPU Intel	24 MB	Minimo: 16 MB Consigliati: 32 MB	Unità CD-ROM
Norton AntiVirus per gateway E-mail Internet	Pentium 133 o superiore	6 MB	32 MB	Unità CD-ROM 500 MB - 5 GB per funzioni di posta ottimali

Tabella 9. Requisiti software per Norton AntiVirus

Componente Intrusion Immunity	**Piattaforme Microsoft Windows**		**OS/2**
	Client	**Server**	**Client**
Norton AntiVirus[1]	Windows NT 4.0 Windows 95, Windows 98	Windows NT 4.0	OS/2 2.11 o versione successiva

Note:

1. Inoltre, è necessaria una connessione Internet TCP/IP per Norton AntiVirus per Internet Email Gateway.

Norton AntiVirus non è disponibile in AIX e Solaris.

Considerazioni sull'installazione di Tivoli Cross-Site for Security

Le seguenti figure illustrano la collocazione tipica degli agenti e del server di gestione di Cross-Site for Security in una rete e-business.

Considerazioni sull'installazione di Norton AntiVirus

Le informazioni relative all'installazione di Norton AntiVirus sono contenute nel file contents.txt nella directory principale del CD del prodotto.

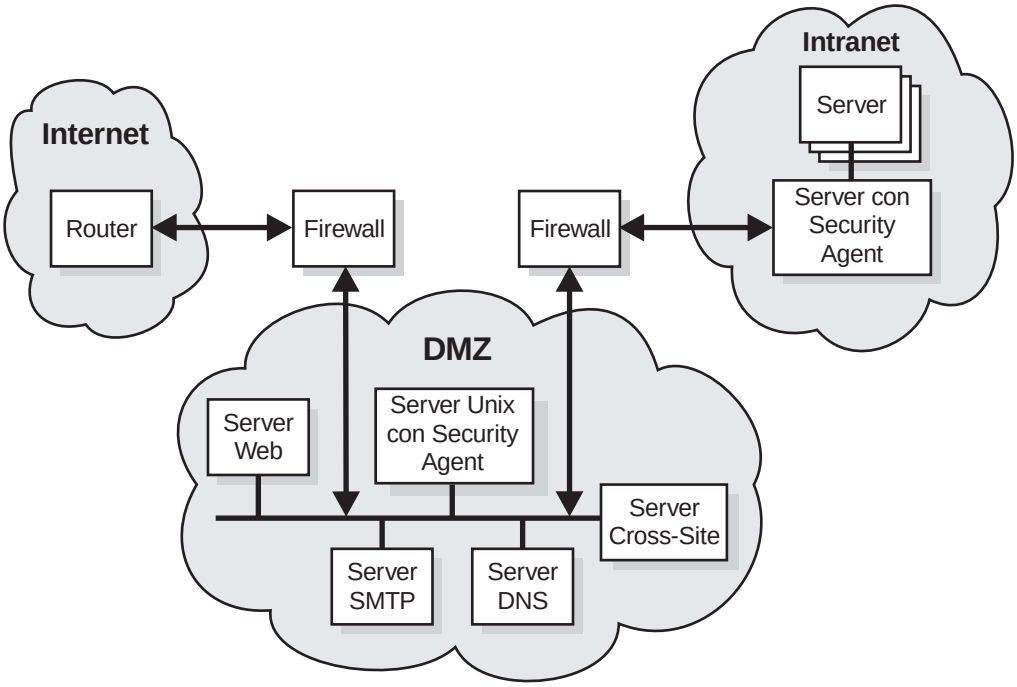


Figura 11. Installazione del server di gestione di Cross-Site for Security in DMZ

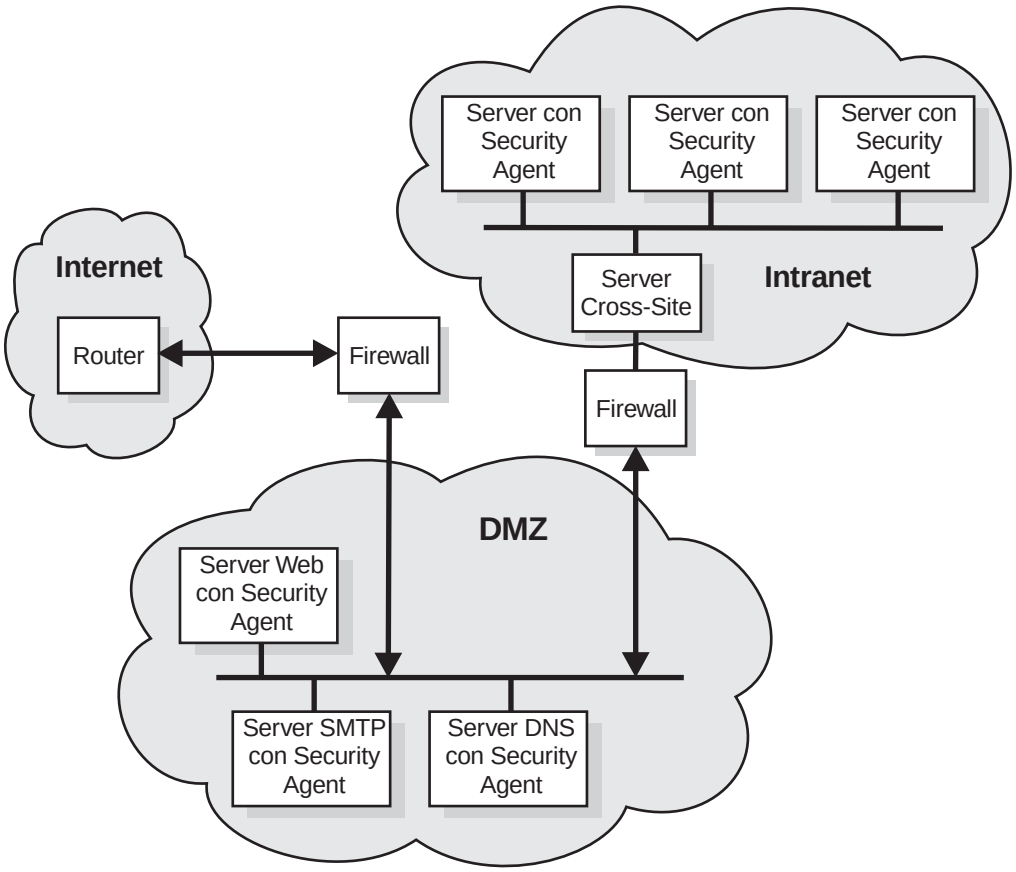


Figura 12. Installazione del server di gestione di Cross-Site for Security nella propria intranet

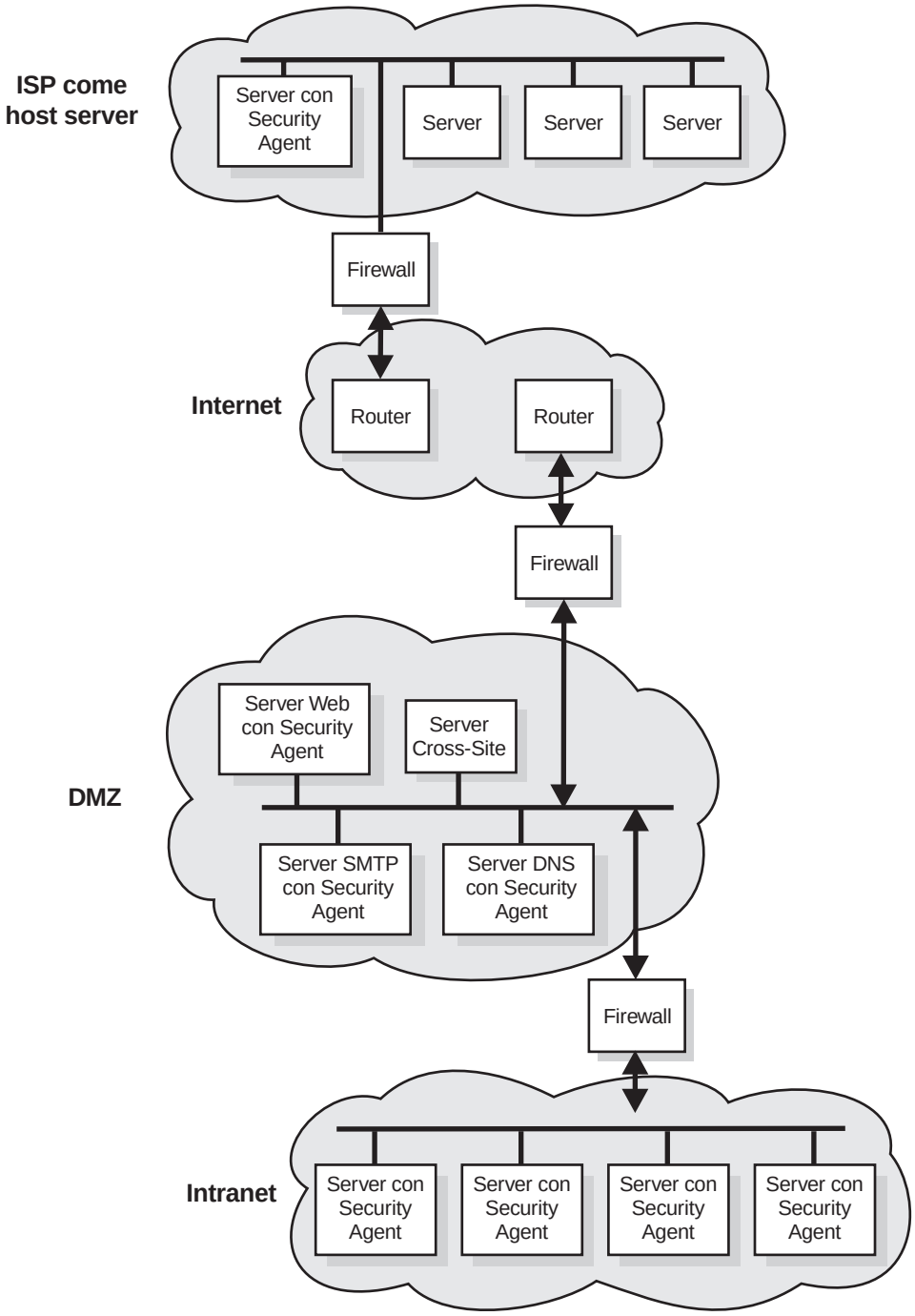


Figura 13. Installazione server di gestione Cross-Site for Security in DMZ che supporta un server collegato a Internet

Capitolo 14. Public Key Infrastructure - Requisiti e considerazioni sull'installazione

Le aziende oggi hanno bisogno di un'infrastruttura con chiave pubblica per proteggere le applicazioni e-business e FirstSecure Trust Authority fornisce due livelli di funzioni che implementano questo tipo di infrastruttura:

- Gestione completa dei certificati digitali che consente:
  - La capacità di richiedere, rinnovare e revocare i certificati
  - Una autorizzazione di registrazione per approvare le richieste certificati
  - Una CA (certificate authority) per la creazione di certificati digitali e di elenchi di revoche
- Capacità di registrazione migliorata per consentire alle aziende di registrare in linea le entità e-business. L'applicazione di registrazione si basa sui seguenti principi:
  - I certificati da emettere e da gestire devono soddisfare i requisiti di convalida richiesti dalle applicazioni e-business più sofisticate e l'autorizzazione deve essere creata per soddisfare tali requisiti di sicurezza e di convalida.
  - L'applicazione deve consentire la flessibilità per supportare un'ampia gamma di politiche di registrazione comprese l'approvazione automatica o manuale, l'autentica flessibile on-site o off-site e l'opzione di isolare le politiche di registrazione in sicuri domini separati.

Il modello di sicurezza garantisce l'accessibilità, la riservatezza, l'integrità e la paternità delle transazioni elettroniche. Mediante la cifratura digitale, la certificazione e la firma, Trust Authority garantisce la protezione delle transazioni e-business in una rete Internet, intranet o in una VPN (virtual private network). Per garantire la riservatezza della propria chiave, la CA (certificate authority) è progettata per funzionare con un hardware cifrato.

Requisiti hardware e software del server Trust Authority

I requisiti software per il server del componente Trust Authority sono elencati nella Tabella 10 a pagina 76.

Tabella 10. Requisiti software e hardware (facoltativi) del server per il componente Public Key Infrastructure Trust Authority

Prodotto	**Note**
Uno dei seguenti sistemi operativi: • IBM AIX/6000 (AIX), Versione 4.3.2 • Microsoft Windows NT, Versione 4.0 con Service Pack 5	• Richiesto. • E' necessario installare tutti i programmi del server di Trust Authority sulla stessa piattaforma. Non è possibile utilizzare sistemi AIX e Windows NT nella stessa configurazione di sistema.
IBM SecureWay Directory Versione 3.1.1	• Richiesto; integrato con il codice di Trust Authority. • Durante l'installazione di Trust Authority, l'utente può scegliere se installare il software Directory sulla stessa macchina su cui viene installato Trust Authority o su una macchina remota.
IBM WebSphere Application Server Versione 2.02, Standard Edition. Include IBM HTTP Server Versione 1.3.3 e JDK (Java Development Kit) della Sun 1.1.7.	• Richiesto; fornito nel pacchetto di supporti di Trust Authority. • Prima di installare Trust Authority, è necessario installare il software del server Web sulla stessa macchina su cui viene installato Trust Authority ed il software del server di Trust Authority.
IBM DB2 Universal Database Enterprise Edition Versione 5.2 con pacchetto di correzioni 9.	• Richiesto; fornito nel pacchetto di supporti di Trust Authority. • Ciascun componente del server dispone di un'istanza di database univoca. Prima di installare Trust Authority, è necessario installare DB2 sulle macchine che si desidera utilizzare come server di Trust Authority.
• IBM SecureWay 4758 PCI Cryptographic Coprocessor, Modello 001 • IBM SecureWay 4758 CCA Support Program, Versione 1.3.0.0 con pacchetto di correzioni 1.3.0.1	• *Facoltativo* e disponibile solo per i sistemi AIX. E' possibile ordinarlo presso la IBM. • Prima di installare Trust Authority, è necessario installare l'hardware 4758 ed il programma di supporto sulla stessa macchina su cui viene installata la CA di Trust Authority. • La scheda di cifratura 4758 richiede un bus PCI su RS/6000.

La Tabella 11 a pagina 77 e la Tabella 12 a pagina 78 contengono i requisiti hardware del server per Trust Authority.

Nella Tabella 11 a pagina 77 e nella Tabella 12 a pagina 78:

- Un ambiente di produzione limitato emette centinaia di certificati al giorno.
- Un ambiente di produzione medio emette migliaia di certificati al giorno.
- Un ambiente di produzione di grandi dimensioni emette diverse migliaia di certificati al giorno. Può inoltre fornire servizi CA per terze parti ad altre organizzazioni.

Se si desidera eseguire Trust Authority in Windows NT, la IBM consiglia di installarlo su un server IBM Netfinity. Nella seguente tabella vengono suggerite le dimensioni

dimensioni da utilizzare per il sistema sulla base del numero di certificati che si prevede di emettere mediante una CA (Certificate Authority) di Trust Authority.

Tabella 11. Configurazione di esempio di Windows NT

Tipo di macchina	**Processori**	**Spazio su disco**	**Memoria**
Ambiente di produzione limitato			
Netfinity 3000	1 (Pentium II a 450 MHz)	2 unità (9,1 GB)	256 MB
Netfinity 5000	2 (Pentium II a 450 MHz)	2 unità (9,1 GB)	512 MB
Ambiente di produzione medio			
Netfinity 3000	1 (Pentium III a 500 MHz)	4 unità (18,2 GB)	768 MB
Netfinity 5000	2 (Pentium III a 500 MHz)	4 unità (9,1 GB)	1 GB
Ambiente di produzione di grandi dimensioni			
Netfinity 5500	2 (Pentium III a 450 MHz)	4 unità (ad alta velocità di 9,1 GB)	1 GB
Netfinity 5500	4 (Pentium III Xeon a 500 MHz con 1024 K di memoria cache L2)	4 unità (ad alta velocità di 9,1 GB)	1 GB
Netfinity 7000	2 (Pentium III a 500 MHz con 512 K di memoria cache L2)	4 unità (ad alta velocità di 9,1 GB)	1 GB
Netfinity 7000	4 (Pentium III Xeon a 500 MHz con 1024 K di memoria cache L2)	4 unità (18,2 GB)	2 GB

Se si desidera eseguire Trust Authority in AIX, è necessario installarlo su una macchina IBM RISC System/6000. Nella seguente tabella vengono suggerite le dimensioni dimensioni da utilizzare per il sistema sulla base del numero di certificati che si prevede di emettere mediante una CA (Certificate Authority) di Trust Authority.

Tabella 12. Configurazione hardware di esempio di un sistema AIX

Tipo di macchina	Processori	Spazio su disco	Memoria
Ambiente di produzione limitato			
F40	2 (233 MHz)	2 unità (9,1 GB, Ultra 2 Fast Wide)	512 MB
Ambiente di produzione medio			
F40	2 (233 MHz)	3 unità (9,1 GB, Ultra 2 Fast Wide)	1 GB
Ambiente di produzione di grandi dimensioni			
F50	4 (332 MHz)	5 unità (una da 9,1 GB Ultra 2 Fast Wide, quattro da 9,1 GB SSA)	2 GB
H50	4 (332 MHz)	5 unità (una da 9,1 GB Ultra 2 Fast Wide, quattro da 9,1 GB SSA)	2 GB
R50	6 (200 MHz)	2 unità (9.1 GB Ultra 2 Fast Wide)	1 GB
R50	8 (200 MHz)	5 unità (una da 9.1 GB Ultra 2 Fast Wide ed una 7133 SSA Rack con quatto SSA da 9.1 GB)	2 GB

Requisiti hardware e software del client di Trust Authority

La IBM consiglia la seguente configurazione della stazione di lavoro per utilizzare i moduli di iscrizione del browser e per eseguire l'applicazione client di Trust Authority.

- Utilizzare la seguente configurazione del sistema:
  - Processore Intel 486 a 166 MHz con almeno 32 MB di memoria (preferibile un processore Intel Pentium a 200 MHz con almeno 64 MB di memoria)
  - Scheda grafica
  - Monitor VGA o superiore
  - Mouse o dispositivo di puntamento compatibile
- Uno dei seguenti sistemi operativi:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT, Versione 4.0
- Uno dei seguenti browser Web:
  - Netscape Navigator oppure Netscape Communicator, Versione 3.0 o successiva

– Microsoft Internet Explorer, Versione 4.0 o successiva, abilitato per Java.

Interazione tra IBM KeyWorks Toolkit e IBM SecureWay Trust Authority

Non installare IBM KeyWorks Toolkit sul server su cui è installato IBM SecureWay Trust Authority.

Capitolo 15. Toolbox - Requisiti e considerazioni sull'installazione

FirstSecure Toolbox è costituita da una serie di API che consentono ad e-business di sviluppare applicazioni sicure.

- Servizi relativi alle autorizzazioni
- Servizi relativi ai certificati e alla gestione
- Servizi di Directory
- Servizi di protocollo Secure Sockets Layer
- Servizi di cifratura e gestione della sicurezza KeyWorks
  - API di IBM Key Recovery Service Provider 1.1.3.0 . IBM Key Recovery Service Provider consente di recuperare le informazioni cifrate.
  - IBM Key Recovery Server 1.1.3.0. IBM Key Recovery Server 1.1.3.0 è un'applicazione che sulla base di una richiesta autorizzata consente di recuperare le informazioni cifrate se le chiavi non sono disponibili, se sono perse o danneggiate.

    Questi due toolkit forniscono delle interfacce standard che possono essere utilizzate dalle applicazioni per richiamare i servizi di sicurezza critici e dai fornitori della sicurezza per utilizzare il toolkit. Le interfacce standard si basano sull'architettura CDSA (Common Data Security Architecture). Questi toolkit sono disponibili in Windows NT, Solaris e AIX.

Requisiti hardware e software di Toolbox

I requisiti hardware per Toolbox vengono illustrati nella Tabella 13.

Tabella 13. Requisiti hardware per Toolbox

Piattaforma	Spazio su disco	Memoria
Versione 4.0, Service Pack 5	2 - 4 GB	64 MB
AIX 4.3.2	9.1 GB	1 GB
Sun Solaris, Versione 2.6 con FixPak del mese di maggio 1999	4.2 GB	128 MB

Tabella 14. Requisiti hardware per i prodotti del componente Toolbox

Toolkit	**Tipo di macchina**	**Spazio su disco**	**Memoria**
IBM KeyWorks Toolkit	Hardware che supporta i prodotti in esecuzione in: Windows NT Versione 4.0, Service Pack 5 o versione successiva Windows 95 AIX 4.2 o versione successiva Sun Solaris	50 MB	32 MB
IBM Key Recovery Service Provider	Hardware che supporta i prodotti in esecuzione in: Windows NT Versione 4.0, Service Pack 5 o versione successiva Windows 95 AIX 4.2 o versione successiva Sun Solaris	50 MB	32 MB

I requisiti software per i prodotti del componente Toolbox sono visualizzati nella tabella riportata di seguito.

Tabella 15. Requisiti software per i prodotti del componente Toolbox

Componente Toolbox	Piattaforme Microsoft Windows		AIX	Solaris
	Client	**Server**	**Server**	**Server**
IBM KeyWorks Toolkit	Windows NT Versione 4.0, Service Pack 5 o versione successiva	Windows NT Versione 4.0, Service Pack 5 o versione successiva Windows 95	AIX 4.2 o versione successiva [1]	Sun Solaris
IBM Key Recovery Service Provider	Windows NT Versione 4.0, Service Pack 5 o versione successiva [2] Windows 95	Windows NT Versione 4.0, Service Pack 5 o versione successiva	AIX 4.2 o versione successiva	Sun Solaris

Note:

1. E' supportato anche AIX client.
2. Inoltre, è richiesto IBM KeyWorks Toolkit.

IBM KeyWorks Toolkit 1.1

IBM KeyWorks Toolkit 1.1 fornisce ai programmatori i mezzi standard, che possono essere utilizzati da aperti per accedere a funzioni cifrate e ad altre funzioni, in diversi ambienti operativi.

IBM KeyWorks Toolkit fornisce le interfacce standard (le API) che possono essere utilizzate dalle applicazioni per richiamare servizi di sicurezza, convalida e crittografia fondamentali, oltre alle interfacce standard che i moduli aggiuntivi del fornitore del servizio possono utilizzare per interfacciarsi al toolkit. Queste interfacce standard si basano su CDSA (Common Data Security Architecture), uno standard della Open Group, sviluppato inizialmente dalla Intel Corporation ed ampliato dalla IBM in KeyWorks Toolkit. Quando si utilizzano le interfacce standard:

- L'azienda può scegliere l'implementazione di convalida e di crittografia che soddisfa meglio i suoi requisiti senza modificare le applicazioni che utilizzano i servizi di sicurezza.
- La produttività dei programmatori di applicazioni e di middleware viene migliorata.

IBM KeyWorks Toolkit fornisce un livello di isolamento tra applicazioni e middleware come classe oltre alle funzioni di cifratura e ai fornitori di servizi. Il toolkit contiene i moduli plug-in del fornitore di servizi e un framework.

Per le applicazioni, il framework fornisce l'API CSSM (Common Security Services Manager) dalla CDSA della Intel Corporation. La IBM ha ampliato l'API CSSM aggiungendo le funzioni di recupero chiavi. Quando si utilizza IBM KeyWorks Toolkit, un'applicazione è im grado di:

- Eseguire la cifratura e annullare la cifratura delle informazioni
- Verificare le firme digitali per diversi scopi
- Richiamare i certificati e gli elenchi di revoca dei certificati dalle directory
- Creare campi di recupero chiavi per il backup della cifratura e il recupero chiavi
- Decidere se convalidare un certificato in base a criteri stabiliti dai programmatori dei sistemi, quando gli utenti emettono un comando

Di solito, un'azienda o OEM integra il toolkit IBM KeyWorks Toolkit e IBM Key Recovery Service Provider con applicazioni e middleware in modo da consentire l'utilizzo delle API CSSM su un Framework CSSM. Il risultato di questa integrazione è una serie di applicazioni runtime e middleware per i server e client distribuiti in ambienti operativi. Gli altri elementi di FirstSecure dipenderanno da IBM KeyWorks Toolkit per tutti i servizi di cifratura e le operazioni delle politiche di convalida.

E' consigliabile che coloro che utilizzano IBM KeyWorks Toolkit per integrare le applicazioni si rivolgano ad un gruppo di ingegneri e di programmatori esperti nella progettazione e nello sviluppo di sistemi di cifratura, di middleware e framework oppure ad OEM dotati di tale esperienza.

Per i fornitori di servizi, framework fornisce l'interfaccia SPI (Service Provider Interface) standard, la CDSA della Open Group. La IBM ha migliorato la SPI aggiungendo le funzioni di recupero chiavi.

IBM KeyWorks Toolkit (SDK) include i moduli plug-in del fornitore di servizi che supportano certificati a chiave pubblica autonomi e a standard aperti. Questi moduli includono PKCS#11, le funzioni di cifratura BSAFE di sicurezza dati RSA, i certificati X.509V3, le politiche di convalida di Entrust, Verisign e LDAP Lightweight Directory Access Protocol. Il framework fornisce un'integrazione autonoma delle funzioni di sicurezza, cifratura e convalida fornita da moduli del fornitore di servizi indipendenti.

IBM KeyWorks Toolkit è in grado di fornire funzioni di gestione primarie, fra cui:

- Protezione dal bypass dei passi vitali in un processo supportato da KeyWorks
- Verifica dei moduli plug-in del fornitore di servizi prima dell'utilizzo per controllare che essi non siano stati modificati
- Utilizzo dei moduli plug-in del fornitore di servizi solo mediante framework
- Supporto per l'utilizzo delle politiche di convalida e di cifratura specifiche per l'azienda o per la nazione

IBM KeyWorks Toolkit garantisce alla propria azienda i seguenti vantaggi:

- Consente di modificare o di sostituire i moduli del fornitore di servizi senza dover riscrivere le applicazioni e il middleware
- Fornisce un supporto autonomo per la cifratura hardware e la firma digitale
- Supporta le directory LDAP e lo standard di firma DSA
- Non richiede l'utilizzo di una particolare CA (Certificate Authority)

Per ulteriori informazioni su IBM KeyWorks Toolkit, consultare il manuale *IBM KeyWorks Toolkit Developer's Guide*.

Interazione tra IBM KeyWorks Toolkit e IBM SecureWay Trust Authority

Non installare IBM KeyWorks Toolkit sul server su cui è installato IBM SecureWay Trust Authority.

IBM Key Recovery Service Provider Toolkit 1.1

IBM Key Recovery Service Provider 1.1.3.0 , fornito in formato toolkit, è un modulo del fornitore di servizi che utilizza le funzioni standard di IBM KeyWorks Toolkit. IBM Key Recovery Service Provider abilita al recupero di informazioni cifrate inviate e memorizzate senza la raccolta e la scrittura di chiavi private e senza la creazione di singoli punti di vulnerabilità della cifratura.

Poiché IBM Key Recovery Service Provider utilizza le funzioni standard fornite da IBM KeyWorks Toolkit, la funzione di recupero chiavi può essere utilizzata con diversi fornitori di cifratura, certificati standard di varie CA (Certificate Authorities), politiche di convalida di Verisign ed Entrust e con qualsiasi directory cui è possibile accedere da LDAP. IBM Key Recovery Service Provider crea le informazioni di recupero chiave in base alla chiave sessione associata alle comunicazioni tra i corrispondenti.

Per ulteriori informazioni su IBM Key Recovery Service Provider, consultare il manuale *Key Recovery Server Installation and Usage Guide*, fornito con la documentazione di FirstSecure.

Capitolo 16. Documentazione fornita con FirstSecure

Ciascun prodotto del componente incluso in FirstSecure è fornito della relativa documentazione. Questo capitolo fornisce le informazioni relative alla documentazione inclusa con ciascun prodotto del componente FirstSecure.

Per SecureWay FirstSecure, SecureWay Policy Director e SecureWay Boundary Server sono disponibili un Media Pack e un pacchetto contenente la documentazione. I Media Pack contengono i CD del prodotto utilizzati per installare i prodotti del componente nell'offerta. Alcuni di essi contengono la documentazione in linea. La documentazione contiene i manuali in formato cartaceo per i prodotti che li forniscono. La sezione “Documentazione di FirstSecure” a pagina 95 contiene l'elenco della documentazione fornita.

Policy Director

Insieme ai prodotti del componente Policy Director viene fornita la seguente documentazione.

IBM SecureWay Policy Director Up and Running
: Contiene informazioni sull'installazione e sulla configurazione di IBM SecureWay Policy Director.

IBM SecureWay Policy Director Administration Guide
: Guida alla gestione di IBM SecureWay Policy Director. Viene fornito in formato PDF.

IBM SecureWay Policy Director Programming Guide and Reference
: Fornisce informazioni per la scrittura di programmi per IBM SecureWay Policy Director. Viene fornito in formato PDF.

Readme del prodotto
: Queste informazioni sono disponibili presso la seguente pagina Web: www.ibm.com/software/security/policy

SecureWay Boundary Server

I seguenti manuali descrivono i prodotti del componente SecureWay Boundary Server, i loro requisiti e le relative interazioni.

IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running
: Manuale in formato cartaceo che descrive i prodotti del componente SecureWay Boundary Server.

Nelle seguenti sezioni viene illustrata la documentazione fornita con i prodotti del componente SecureWay Boundary Server.

IBM SecureWay Firewall

Tutta la documentazione di IBM Firewall viene fornita in formato elettronico. IBM Firewall include la seguente documentazione:

IBM SecureWay Firewall for AIX Setup and Installation
: Istruzioni per l'installazione e la configurazione di IBM SecureWay Firewall per AIX.

IBM SecureWay Firewall for Windows NT Setup and Installation
: Istruzioni per l'installazione e la configurazione di IBM SecureWay Firewall per Windows NT.

IBM SecureWay Firewall for AIX User's Guide
: Istruzioni per l'installazione e la configurazione di IBM SecureWay Firewall per Windows NT.

IBM SecureWay Firewall for Windows NT User's Guide
: Informazioni sull'utilizzo di IBM Firewall per Windows NT.

IBM SecureWay Firewall for Windows NT Reference
: Contiene il materiale di riferimento per l'utilizzo di IBM Firewall per Windows NT.

IBM SecureWay Firewall for AIX Reference
: Contiene il materiale di riferimento per l'utilizzo di IBM Firewall per AIX.

IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX
: Contiene le istruzioni necessarie per la determinazione dei problemi.

IBM SecureWay Firewall VPN Client User's Guide
: Fornisce informazioni sull'utilizzo e sulla configurazione di una rete privata virtuale.

MIMEsweeper

MIMEsweeper include la seguente documentazione:

MIMEsweeper Administrator's Guide
: Contiene una sezione Release Notes, seguita dalle informazioni per il responsabile, comprese quelle di installazione e di pianificazione.

  Questo manuale viene fornito in formato HTML sul CD del prodotto. E' possibile visualizzarlo in linea, utilizzando un browser Web per visualizzare il file denominato \DOC\MANUAL.HTM.

MIMEsweeper Release Notes
: Contiene la documentazione aggiornata, comprese le informazioni di installazione e le istruzioni per la visualizzazione in linea della documentazione.

  Questo manuale viene fornito in formato HTML sul CD del prodotto. E' possibile visualizzarlo in linea, utilizzando un browser Web per visualizzare il file denominato \DOC\RELNOTES.HTM.

MIMEsweeper Configuration Editor Help
: Contiene informazioni relative alla modifica dei file di configurazione di MIMEsweeper.

  Questo documento viene fornito in formato HTML sul CD del prodotto.

SurfinGate

SurfinGate contiene la seguente documentazione in formato elettronico:

SurfinGate Installation Guide
: Contiene informazioni sull'installazione e sulla configurazione dei componenti di SurfinGate 4.05 in Windows NT. La versione in formato PDF del manuale *SurfinGate Installation Guide* è contenuta nel seguente file nel CD del prodotto: \docs\install.pdf.

SurfinGate User Guide
: Contiene informazioni sulla pianificazione e sull'utilizzo di SurfinGate. Una versione PDF della pubblicazione *SurfinGate User Guide* viene fornita sul CD del prodotto nel file: \docs\manual.pdf.

SurfinGate 4.05 for Windows NT Release Notes
: Contiene informazioni su SurfinGate 4.05, inclusi i requisiti di sistema e le limitazioni del prodotto. Una versione in formato PDF del manuale *SurfinGate 4.05 for Windows NT Release Notes* è contenuta nel seguente file nel CD del prodotto: \docs\relnotes.pdf.

SurfinGate for Windows NT/UNIX Solaris Release Notes, Appendix A
: Documento in linea che illustra le modifiche apportate in SurfinGate. E' contenuto nel seguente file nel CD del prodotto: \docs\rnappen.pdf.

Intrusion Immunity

Le sezioni seguenti descrivono la documentazione fornita con il prodotto del componente Intrusion Immunity.

Tivoli Cross-Site for Security

Tivoli Cross-Site per Security, Versione 1.1 contiene le seguente documentazione in formato .pdf:

Tivoli Cross-Site for Security Installation
: Fornisce informazioni dettagliate sui requisiti di installazione e guida l'utente nella procedura di installazione.

Tivoli Cross-Site for Security User's Guide
: Contiene una panoramica del prodotto, le informazioni per l'utilizzo della console e per l'esecuzione delle attività, informazioni di riferimento sulle interfacce della riga comandi, sui file di configurazione e un glossario. E' possibile accedere a questo documento mediante il CD-ROM del prodotto.

Norton AntiVirus

Norton AntiVirus include la seguente documentazione per i componenti supportati in FirstSecure. Tutti i documenti, escluso il file contents.txt vengono forniti in formato PDF sul CD di Norton AntiVirus. Il file contents.txt è un file ASCII contenuto nel CD del prodotto.

Documentazione contenuta nel CD di Norton AntiVirus Solution Rilascio 3.04

Il file nel CD di Norton AntiVirus Solution Rilascio 3.04 denominato \contents.txt contiene la documentazione inserita nel CD.

Soluzioni di gestione

Norton AntiVirus Solution Implementation Guide
: Consultare il file \docs\admin\navimp.pdf nel CD del prodotto.

Norton AntiVirus Command-Line Scanner
: Consultare il file \docs\navc\navcugd.pdf nel CD del prodotto.

Emergency Rescue Disk creation
: Consultare il file \navc\readme.txt nel CD del prodotto.

Soluzioni per il server

Norton AntiVirus for Windows NT Server Administrator's Guide
Consultare il file \docs\admin\navnts50.pdf nel CD del prodotto.

Norton AntiVirus for NetWare User's Guide
Consultare il file \docs\NAVNLM\NVN4.pdf nel CD del prodotto.

Norton AntiVirus for Lotus Notes Installation Guide
Consultare il file \docs\NAVNOTES\NAVNOTES.pdf nel CD del prodotto.

Norton AntiVirus for Lotus Notes Installation Guide
Consultare il file \docs\NAVNOTES\NAVNOTES.pdf nel CD del prodotto.

Norton AntiVirus for OS/2 Lotus Notes Installation Guide
Consultare il file \docs\NOTESOS2\NOTESOS2.pdf nel CD del prodotto.

Norton AntiVirus for Microsoft Exchange Installation Guide
Consultare il file \docs\NAVXCHNG\NAVXCHNG.pdf nel CD del prodotto.

Soluzioni per il gateway

Norton AntiVirus for Internet Email Gateway User's Guide
Consultare il file \docs\navieg\navieg.pdf nel CD del prodotto.

Norton AntiVirus for Firewalls Administrator's Guide
Consultare il file \docs\navfw\navfw.pdf nel CD del prodotto.

Soluzioni per il desktop

Norton AntiVirus User's Guide for Windows 3.1/DOS
Consultare il file \docs\navwks\nav4dusr.pdf nel CD del prodotto.

Norton AntiVirus Reference Guide for Windows 3.1/DOS
Consultare il file \docs\navwks\nav4dref.pdf nel CD del prodotto.

Norton AntiVirus for Windows 95/98 User's Guide
Consultare il file \docs\navwks\nav98usr.pdf nel CD del prodotto.

Norton AntiVirus for Windows 95/98 Reference Guide
Consultare il file \docs\navwks\nav98ref.pdf nel CD del prodotto.

Norton AntiVirus for Windows NT User's Guide
Consultare il file \docs\navwks\nav5nusr.pdf nel CD del prodotto.

Norton AntiVirus for Windows NT Reference Guide
Consultare il file \docs\navwks\nav5nref.pdf nel CD del prodotto.

Norton AntiVirus v4.0 User's Guide for Windows NT
Consultare il file \docs\351\navntugd.pdf nel CD del prodotto.

Norton AntiVirus v4.0 Reference Guide for Windows NT
Consultare il file \docs\351\navntref.pdf nel CD del prodotto.

Norton AntiVirus User's Guide for OS/2
Consultare il file \docs\navos2\navos2ug.pdf nel CD del prodotto.

Norton AntiVirus Distribution Guide for OS/2
Consultare il file \docs\navos2\navos2dg.pdf nel CD del prodotto.

Norton AntiVirus for Macintosh User's Guide
Consultare il file \docs\navmac\navmac.pdf nel CD del prodotto.

White papers nel CD di Norton AntiVirus Solution Rilascio 3.04: Il CD contiene inoltre delle White papers nella directory \sarc. Ognuna di esse è in formato .pdf.

Video contenuti nel CD di Norton AntiVirus Solution Rilascio 3.04: Il CD contiene dei video. Per visualizzarli, è necessario disporre di un Lettore multimediale o di un altro programma in grado di riprodurre i file .AVI. I video sono contenuti nei seguenti file:

SARC \sarc\sarc.avi

About Viruses
\sarc\aboutvir.avi

Norton AntiVirus: the Guided Tour
\navtour\guided\demo32.exe

How to Respond When Norton AntiVirus Alerts You
\navtour\alert\demo32.exe

A Tour of Norton System Center
\nsctour\setup.exe

oppure, per avviare il file direttamente dal CD,

\nsctour\demo32.exe

Per ulteriori informazioni, consultare il file \ncstour\readme.txt

Trust Authority

La documentazione del prodotto IBM SecureWay Trust Authority è disponibile in formato PDF (Portable Document Format) e HTML nel CD-ROM della documentazione di *Trust Authority*. La maggior parte della documentazione è stata tradotta nelle lingue supportate da Trust Authority. Per informazioni su come accedere ad un manuale in una determinata lingua, consultare il file *Readme* del prodotto. La versione più aggiornata del file *Readme* è disponibile nella pagina Library del sito Web di IBM SecureWay Trust Authority all'indirizzo http://www.ibm.com/software/security/trust/library

La libreria di Trust Authority contiene la seguente documentazione:

IBM SecureWay Trust Authority Up and Running
Fornisce una panoramica del prodotto. Elenca i requisiti del prodotto, illustra le procedure di installazione e le modalità di accesso alla guida in linea disponibile per ciascun componente del prodotto. Oltre ad essere inserito nel

CD della *Documentazione*, il manuale viene fornito in formato cartaceo insieme al prodotto.

IBM SecureWay Trust Authority System Administration Guide
: Contiene informazioni di carattere generale sulla gestione del sistema Trust Authority. Illustra le procedure cui attenersi per le seguenti attività: avvio e chiusura dei server, modifica delle password, gestione della CA (Certificate Authority), esecuzione di audit e di verifiche dell'integrità dei dati.

IBM SecureWay Trust Authority Configuration Guide
: Contiene informazioni sull'utilizzo di Procedura guidata di configurazione per configurare un sistema Trust Authority. L'utente può accedere alla versione HTML di questo manuale mediante la guida in linea del Wizard.

IBM SecureWay Trust Authority Registration Authority Desktop Guide
: Contiene informazioni sull'utilizzo di RA Desktop per gestire i certificati nel periodo di validità di questi ultimi. L'utente può accedere alla versione HTML di questo manuale mediante la guida in linea del Desktop.

IBM SecureWay Trust Authority User's Guide
: Contiene le istruzioni necessarie per ottenere i certificati. Guida all'utilizzo dei moduli di iscrizione di Trust Authority per richiedere i certificati per i browser, i server e le unità. Fornisce istruzioni su come registrarsi in anticipo per un certificato PKIX e su come utilizzare il client di Trust Authority per memorizzare e gestire i certificati PKIX. L'utente può accedere alla versione HTML di questo manuale mediante la guida in linea del Client.

Toolbox

Le sezioni seguenti descrivono la documentazione fornita con i prodotti del componente Toolbox.

Le API di Toolbox

La documentazione di Toolbox è disponibile presso il seguente sito Web: `www.ibm.com/software/security/firstsecure/library`. Sono disponibili i seguenti manuali:

IBM SecureWay Secure Sockets Layer Toolkit Programming Guide and Reference
: Fornisce una panoramica delle API e di iKeyman. Definisce le singole API, la relativa sintassi e l'utilizzo.

IBM SecureWay Directory Client SDK Programming Reference
: Contiene una serie di programmi per il client LDAP di esempio e una libreria del client LDAP che consentono di accedere alle applicazioni sui server LDAP. Viene fornito il supporto per C e Java.

IBM SecureWay Policy Director Programming Guide and Reference
Definisce le singole API, la relativa sintassi e l'utilizzo.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Installation Guide
Fornisce i requisiti e le istruzioni di installazione.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference
Contiene informazioni per i programmatori che sviluppano le applicazioni mediante IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms, noto anche come PKIX. Fornisce una panoramica del prodotto, istruzioni per la scrittura di programmi per i singoli componenti di PKIX e una descrizione delle API di PKIX.

IBM KeyWorks Toolkit

Tutta la documentazione fornita con IBM KeyWorks Toolkit è in linea, in formato PDF e si trova sul CD del prodotto. La documentazione è la seguente:

IBM KeyWorks Toolkit Developer's Guide
Fornisce una panoramica del toolkit. Indica inoltre, le modalità di integrazione del toolkit nelle applicazioni e contiene un'applicazione di esempio.

IBM KeyWorks Toolkit Application Programming Interface (API) Specification
Definisce l'interfaccia che i programmatori utilizzano per accedere ai servizi di sicurezza forniti dai moduli del fornitore di servizi e framework.

IBM KeyWorks Toolkit Service Provider Module Structure & Administration
Descrive le funzioni comuni a tutti i moduli del fornitore dei servizi toolkit. Questo documento va utilizzato insieme alle specifica di interfaccia del fornitore di servizi individuali per la creazione di un modulo del fornitore di servizi.

IBM KeyWorks Toolkit Cryptographic Service Provider Interface Specification
Definisce l'interfaccia a cui i moduli del fornitore di servizi di cifratura deve conformarsi per poter essere accessibile dal toolkit.

IBM Key Recovery Service Provider Interface (KRSPI) Specification
Definisce l'interfaccia a cui i moduli del fornitore di servizi di recupero chiavi deve conformarsi per poter essere accessibile dal toolkit.

IBM KeyWorks Toolkit Trust Policy Interface Specification
Definisce l'interfaccia a cui gli sviluppatori delle politiche, come ad esempio i programmatori di applicazioni che creano le politiche, i certificati e le CA (Certificate Authorities), devono conformarsi per poter estendere il toolkit con il modello o le politiche specifiche dell'applicazione.

IBM KeyWorks Toolkit Certificate Library Interface (CLI) Specification
Definisce l'interfaccia a cui i programmatori della libreria certificati devono conformarsi per fornire servizi di gestione certificati specifici del formato a varie applicazioni toolkit e moduli di politiche convalidate.

IBM KeyWorks Toolkit Data Storage Library Interface (DLI) Specification
: Definisce l'interfaccia a cui i programmatori della libreria devono conformarsi per fornire memorizzazioni di certificati congruenti e indipendenti dal formato o specifiche del formato.

IBM Key Recovery Service Provider

La documentazione seguente viene fornita con IBM Key Recovery Service Provider in formato PDF nel CD del prodotto:

IBM Key Recovery Service Provider Key Recovery Server Installation and Usage Guide
: Fornisce una spiegazione dei concetti di recupero chiavi, una guida nell'impostazione della soluzione di recupero chiavi per un'azienda e le procedure per l'installazione, la configurazione e l'esecuzione di IBM Key Recovery Server.

Redbook sulla sicurezza

I Redbook elencati di seguito, prodotti dalla ITSO (IBM International Technical Support Organization), forniscono informazioni sui processi e sui prodotti relativi alla sicurezza. Sono disponibili all'indirizzo www.us.ibm.com/redbooks.

- Understanding the IBM SecureWay FirstSecure Framework
- *High Availability IBM eNetwork Firewall*

Documentazione

Per IBM SecureWay FirstSecure è disponibile la documentazione elencata di seguito.

Documentazione di FirstSecure

La documentazione di FirstSecure contiene i seguenti manuali:

- FirstSecure License Information
- *IBM SecureWay FirstSecure Planning and Integration*
- *IBM SecureWay Policy Director Up and Running*
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*

- *IBM SecureWay Trust Authority Up and Running*
- *Tivoli Cross-Site for Security Installation*

Documentazione di Policy Director

La documentazione di Policy Director contiene i seguenti manuali:

- Policy Director License Information
- *IBM SecureWay Policy Director Up and Running*

Documentazione di SecureWay Boundary Server

La documentazione di SecureWay Boundary Server contiene i seguenti manuali:

- SecureWay Boundary Server License Information
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*

Parte 4. Appendici

Appendice A. Informazioni particolari

Queste informazioni sono state sviluppate per i prodotti e i servizi offerti negli Stati Uniti. E' possibile che negli altri paesi l'IBM non offra i prodotti, le funzioni o i servizi illustrati in questo documento. Consultare il rappresentante IBM locale per informazioni sui prodotti e sui servizi disponibili nel proprio paese. Ogni riferimento relativo a prodotti, programmi o servizi IBM non implica che solo quei prodotti, programmi o servizi IBM possano essere utilizzati. In sostituzione a quelli forniti dall'IBM, possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino violazione dei diritti di proprietà intellettuale o di altri diritti dell'IBM. E' comunque responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri prodotti, programmi o servizi non IBM.

L'IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nella presente pubblicazione. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su di essi. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

IBM Director of Commercial Relations
IBM Corporation
Schoenaicher Str. 220,
D-7030 Boeblingen
Deutschland

Il seguente paragrafo non e' valido per il Regno Unito o per tutti i paesi le cui leggi nazionali siano in contrasto con le disposizioni in esso contenute: L'IBM FORNISCE QUESTA PUBBLICAZIONE NELLO STATO IN CUI SI TROVA SENZA ALCUNA GARANZIA, ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIABILITA' ED IDONEITA' AD UNO SCOPO SPECIFICO. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, quindi, la presente dichiarazione potrebbe non essere a voi applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate su base periodica; tali modifiche verranno incorporate nelle nuove edizioni della pubblicazione. L'IBM si riserva il diritto di apportare miglioramenti e/o modifiche al prodotto o al programma descritto nel manuale in qualsiasi momento e senza preavviso.

Tutti i riferimenti a siti Web non dell'IBM contenuti in questa pubblicazione sono forniti unicamente a scopo di consultazione. I materiali contenuti in tali siti Web non fanno parte di questo prodotto e l'utente si assume ogni rischio relativo al loro utilizzo.

L'IBM può utilizzare o divulgare le informazioni ricevute dagli utenti secondo le modalità ritenute appropriate, senza alcun obbligo nei loro confronti.

Coloro che detengono la licenza su questo programma e desiderano avere informazioni allo scopo di consentire: (i) uno scambio di informazioni tra programmi indipendenti e altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Queste informazioni possono essere rese disponibili, secondo condizioni contrattuali appropriate, compreso, in alcuni casi, il pagamento di un addebito.

Il programma su licenza descritto in questo manuale e tutto il materiale su licenza ad esso relativo sono forniti dall'IBM nel rispetto delle condizioni previste dalla licenza d'uso.

Qualsiasi informazione relativa alle prestazioni è stata verificata in un ambiente controllato. Di conseguenza l'utilizzo del prodotto in ambienti operativi diversi può comportare risultati sensibilmente diversi. Alcune rilevazioni possono essere state effettuate su sistemi a livello di sviluppo e non si garantisce in alcun modo, dunque, che siano uguali alle rilevazioni eseguite sui vari sistemi disponibili. Inoltre, è possibile che ad alcune di queste rilevazioni si sia pervenuti tramite estrapolazione. I risultati attuali potrebbero variare. E' necessario che gli utenti confrontino i dati in base agli ambienti utilizzati.

Le informazioni relative a prodotti non IBM sono state ottenute dai fornitori di tali prodotti. L'IBM non ha verificato tali prodotti e non può garantirne l'accuratezza delle prestazioni. Eventuali reclami relativi a questi prodotti devono essere inviati ai fornitori degli stessi.

Le dichiarazioni relative a futuri intenti o obiettivi IBM sono soggette a modifiche senza preavviso.

Queste informazioni sono unicamente a scopo di pianificazione. Potrebbero essere modificate prima che i prodotti descritti siano resi disponibili.

Marchi

I seguenti termini sono marchi dell'IBM (International Business Machines Corporation) negli Stati Uniti o in altri paesi o in entrambi:

AIX
AIX/6000
DB2

DB2 Universal Database
eNetwork
Global Sign-On
GSO
IBM
Netfinity
OS/2
RS/6000
SecureWay
Websphere

Intel e Pentium sono marchi della Intel Corporation.

Java e tutti i marchi e logo basati su Java sono marchi della Sun Microsystems, Inc..

Lotus, Lotus Notes, Domino e cc:Mail sono marchi della Lotus Development Corporation.

Microsoft, Windows, Windows NT ed il logo di Windows sono marchi della Microsoft Corporation.

Tivoli è un marchio della Tivoli Systems Inc..

UNIX è un marchio fornito su licenza esclusivamente mediante la X/Open Company Limited.

Nomi di altri prodotti, società e servizi, possono essere marchi di altre società.

Glossario

Questo glossario definisce i termini e le abbreviazioni utilizzate in questo manuale, alcuni dei quali potrebbero essere nuovi, di uso non comune e di particolare interesse. Include termini e definizioni tratte da:

- The IBM Dictionary of Computing, New York: McGraw-Hill, 1994.
- The American National Standard Dictionary for Information Systems, ANSI X3.172–1990, American National Standards Institute (ANSI), 1990.
- The Answers to Frequently Asked Questions, Version 3.0, California: RSA Data Security, Inc., 1996.

.

A

ACL. ACL (Access Control List), elenco di controllo degli accessi.

ACL (access control list). Un meccanismo che limita l'utilizzo di risorse specifiche a utenti autorizzati.

ActiveX. Una serie di termini e tecnologie ad oggetti utilizzati nei linguaggi di programmazione Microsoft.

agente. In Tivoli Cross-Site for Security, un programma di controllo dei pacchetti IP, che raccoglie i pacchetti e ne controlla le anomalie su diversi livelli della rete e che mantiene traccia delle statistiche e degli stati delle connessioni stabilite.

API. API (Application programming interface).

API (application program interface). Un'interfaccia funzionale che consente ad un programma scritto in un linguaggio di alto livello, di utilizzare funzioni specifiche.

Applet. Un programma scritto in Java che viene eseguito nei browser compatibili con Java, come ad esempio, Netscape Navigator. Noto anche come applet Java.

Applicazione Web. Un applicazione progettata per accedere al Word Wide Web.

autenticazione. Il processo di affidabilità che determina l'identità delle parti durante le comunicazioni.

autorita' per la certificazione. L'entità, l'applicazione software o le persone responsabili dell'applicazione delle politiche di sicurezza di un'organizzazione e dell'assegnazione di identità elettroniche di sicurezza in formato di certificati. L'autorizzazione certificati elabora le richieste di emissione, rinnovo e revoca dei certificati.

Autorizzazione. Il processo che determina i tipi di attività consentiti per l'utilizzo da parte di un utente. Di norma, l'autorizzazione si verifica in seguito ad un'autenticazione.

B

Bloodhound. In Norton AntiVirus, il componente che rileva un virus.

bomba macro. Una sequenza di comandi salvati inviata ad un altro utente per provocare risultati indesiderati.

Browser Web. Il software client eseguito sul proprio PC e che consente la navigazione in Internet o di pagine locali. E' uno strumento di richiamo che consente di accedere universalmente ad una ampia raccolta di materiale ipermediale disponibile sul Web e su Internet. Esempi tipici di browser sono Netscape Navigator e Microsoft Internet Explorer. *Consultare anche* server.

C

Canale. Un percorso su cui i segnali possono essere inviati.

cella. In DCE, un gruppo di utenti, sistemi e risorse che sono di solito riunite con uno scopo comune e che condividono la sicurezza, la gestione e i limiti di denominazione. Di solito, una cella e formata da utenti, macchine e risorse che dividono uno scopo comune e che hanno un livello di fiducia più' elevato tra loro, rispetto a quello che hanno con utenti, macchine e risorse, che non condividono la cella.

Cell directory service. Un componente di DCE (Distributed Computing Environment) che gestisce un

database di informazioni relative a risorse che si trovano in una cella DCE.

Certificato digitale. Una credenziale elettronica emessa ad una persona o entità, da una terza parte convalidata. Un certificato contiene informazioni relative all'entità per la quale il certificato viene emesso.

chiave pubblica. La chiave in una coppia di chiavi pubblica/privata resa disponibile ad altri utenti. Li abilita ad indirizzare una transazione al proprietario della chiave o a verificare una firma digitale. I dati cifrati con una chiave pubblica possono essere decodificati solo col la corrispondente chiave privata. *Consultare anche*coppia di chiavi pubblica/privata.

Client. (1) Un'unità funzionale che riceve i servizi condivisi da un server. (2) Un programma o computer che richiede un servizio di un altro computer o programma.

codice mobile. Fa riferimento al calcolo eseguito su un computer portatile da un utente che si sposta spesso tra diverse località e che utilizza diversi tipi di collegamenti di rete (ad esempio, dial-up, LAN o senza fili).

codifica. Codificare le informazioni in modo che soltanto chi conosca l'appropriato codice di decodifica, possa riottenere le informazioni originali tramite decodifica.

Controllo accessi. Nella sicurezza dei computer, il processo che assicura che le risorse di un sistema possano essere accedute solo da utenti autorizzati e in modi autorizzati.

coppia di chiavi pubblica/privata. Una coppia di chiavi pubblica/privata fa parte del concetto di cifratura delle coppie di chiavi (introdotto nel 1976 da Diffie e da Hellman per risolvere il problema di gestione delle chiavi). Nel loro concetto, ciascuna persona ottiene una coppia di chiavi, una denominata pubblica e l'altra privata. Ciascuna chiave pubblica di una persona è resa pubblica mentre la privata viene mantenuta segreta. Il mittente ed il destinatario non devono condividere informazioni segrete: tutte le comunicazioni coinvolgono solo le chiavi pubbliche, le chiavi private non vengono mai trasmesse o condivise. Non è quindi più necessario convalidare il canale di comunicazione per proteggersi da truffe e perdita di dati. Il solo requisito richiesto è che le chiavi pubbliche vengano associate ai rispettivi utenti in un nodo convalidato (autenticato), ad esempio in una directory convalidata. Chiunque può inviare un messaggio riservato utilizzando informazioni pubbliche. Tuttavia, il messaggio può essere decodificato solo da una chiave privata, in possesso del destinatario previsto. Quindi, la cifratura della coppia di chiavi può essere utilizzata non solo per la riservatezza (cifratura) ma anche per l'autenticazione (firme digitali).

D

daemon. In AIX, un programma che resta residente in attesa di eseguire un servizio.

DCE. DCE (Distributed Computing Environment).

DCE (Distributed Computing Environment). Servizi e strumenti che supportano la creazione, l'utilizzo e la gestione, di applicazioni distribuite in un ambiente di calcolo eterogeneo.

E

e-business. L'esecuzione di transazioni commerciali tra le reti e computer. Include l'acquisto e la vendita di beni e servizi. Include inoltre, il trasferimento di fondi mediante comunicazioni digitali.

e-commerce. L'esecuzione di transazioni tra società. Include l'acquisto e la vendita di beni e servizi (utilizzando clienti, fornitori, rivendite e altro), su Internet. E' un elemento fondamentale di e-business.

extranet. Una derivazione di Internet che utilizza tecnologie simili. Le società stanno iniziando ad applicare la pubblicazione Web, il commercio elettronico, la distribuzione dei messaggi e il raggruppamento di clienti, partner e personale interno.

F

filtro contenuto. Disassemblare una trasmissione per leggerne i contenuti in modo da determinare se la trasmissione soddisfa gli standard di contenuti specifici.

filtro degli indirizzi di rete. Il processo di verifica dell'indirizzo della posta in entrata ed uscita per controllare se il destinatario o il mittente sono validi.

firewall. Un sistema o una combinazione di sistemi che rafforzano le barriere tra due o più reti.

FTP (File Transfer Protocol). Un protocollo client/server di Internet che può essere utilizzato per trasferire i file tra computer.

G

gateway. Un sistema che consente a reti incompatibili o applicazioni incompatibili di comunicare tra loro.

Gateway a livello circuito. In un firewall, un proxy server che reindirizza una richiesta client nel firewall in direzione del server specificato.

H

hacker. Una persona che tenta di accedere ad una macchina o sistema senza l'apposita autorizzazione. Gli hacker di solito, tendono ad utilizzare le risorse senza averne il permesso.

heartbeat. Una comunicazione fra un programma e un programma di gestione per confermare un'attività, il programma comunica al programma di gestione che è ancora attivo eseguendo la propria attività.

I

IDE. IDE (Integrated development environment).

IDE (integrated development environment). Un programma per lo sviluppo di applicazioni che consente di creare il codice delle applicazioni, eseguirle senza punti di interruzione e ricevere l'aiuto diagnostico per gli errori di programma.

incidente. In Tivoli Cross-Site for Security, un'attività sospetta che potrebbe attaccare il sistema.

Internet. Una raccolta mondiale di reti che consente le comunicazioni elettroniche tra computer. Li abilita a comunicare tra loro mediante dispositivi software, come ad esempio la posta elettronica o i browser Web. Ad esempio, alcune università sono su una rete che a sua volta, sono collegate a reti simili per formare Internet.

intranet. Una rete che si trova all'interno di una azienda che spesso si trova dietro firewall. E' una derivazione di Internet che utilizza tecnologie simili. Tecnicamente, Intranet è una estensione di Internet. HTML (un linguaggio utilizzato per la rappresentazione grafica delle informazioni) e HTTP (un protocollo che trasferisce i file ipertestuali su Internet) sono alcuni dei punti in comune.

IntraVerse server. In IntraVerse, un sistema sulla rete che contiene il software server IntraVerse e che può comunicare con tutti i sistemi host che sono in esecuzione sul software client di NetSEAT. IntraVerse server fa riferimento ad un sistema o ad una combinazione di sistemi che ne eseguono i relativi programmi.

IPSec. Uno standard IPS (Internet Protocol Security) sviluppato da IETF. IPSec è un protocollo di livello reti progettato per fornire i servizi di sicurezza cifrata che supportano in modo flessibile le combinazioni di autenticazione, integrità, controllo degli accessi e riservatezza. Per le sue potenti funzioni di autenticazione, è stato utilizzato da molti rivenditori di prodotti VPN come protocollo per stabilire connessioni sicure da un punto ad un altro di Internet.

ISV. ISV (Independent Software Vendor).

J

Java. Una serie di tecnologie per la rete, indipendente dal sistema di computer utilizzato, sviluppata dalla Sun Microsystems, Incorporated. L'ambiente Java è formato dal sistema operativo Java, le macchine virtuali per le diverse piattaforme, il linguaggio di programmazione ad oggetti Java e da diverse librerie di classe.

JavaScript. Un linguaggio di script simile a Java sviluppato dalla Netscape per essere utilizzato con i suoi browser.

K

Kerberos. Un metodo di sicurezza per l'autenticazione di un servizio che esegue una richiesta di un computer. Kerberos è stato sviluppato per l'Athena Project presso il MIT (Massachusetts Institute of Technology). Nella mitologia greca, Kerberos era un cane a tre teste che sorvegliava i cancelli di Hades. Kerberos fornisce ad una richiesta utente un cartellino cifrato da un processo di autenticazione che può essere utilizzato per richiedere un servizio specificato da un server. La password dell'utente non richiede alcun permesso di entrata nella rete.

L

LDAP. LDAP (Lightweight Directory Access Protocol).

Lightweight Directory Access Protocol. In IBM SecureWay Directory, LDAP fornisce un modo per conservare le informazioni di directory in una ubicazione centrale, per la memorizzazione, l'aggiornamento, il richiamo e lo scambio.

M

MPEG. Lo standard in fase di sviluppo da parte del MPEG (Moving Pictures Experts Group) per la compressione e la memorizzazione di immagini in movimento ed animazioni in formato digitale.

N

namespace. Riferita alla Directory, la struttura esterna dei nomi accessibili dagli utenti.

non negazione. L'utilizzo di una chiave privata digitale per impedire che il firmatario di un documento possa falsamente negare di averlo firmato.

O

OEM. OEM (Original equipment manufacturer).

Oggetto Web. I dati resi disponibili mediante un browser Web. Un oggetto Web può essere una pagina Web, una sua parte, un file, un immagine, una directory, un programma CGI o un applet Java.

ORB (object request broker). Nella programmazione ad oggetti, il software che agisce come intermediario abilitando, in modo trasparente, gli oggetti allo scambio di richieste e risposte.

P

plug-in. Un programma che può essere utilizzato come parte di un browser Web.

principale. In DCE, l'entità che può comunicare in modo sicuro con un'altra entità mediante la sicurezza DCE. I principali possono essere utenti, server o computer.

proxy server. L'intermediario tra il computer che richiede l'accesso (A) e quello cui si accede (B). Quindi, se un utente finale effettua una richiesta di una risorsa dal computer A, questa richiesta viene indirizzata ad un proxy server. Il proxy server effettua la richiesta, ottiene la risposta dal computer B e quindi la inoltra all'utente finale. I proxy server sono utili per accedere ad Internet da un firewall.

R

RPC. In DCE, una RPC (remote procedure call)

RPC (remote procedure call). (1) Una funzione utilizzata da un client per richiedere l'esecuzione di una chiamata di procedura da un server. Questa funzione include una libreria delle procedure ed una rappresentazione dati esterna. (2) Una richiesta client ad un fornitore di servizi ubicato in un altro nodo.

S

server. (1) In una rete, una stazione di dati che fornisce le funzioni ad altre stazioni, ad esempio un server di file. (2) In TCP/IP, un sistema in una rete che gestisce le richieste di un sistema verso un altro sito, denominato client/server.

server Apache. Una serie di software server Web disponibili gratuitamente.

server socks. Un gateway a livello circuito che fornisce un collegamento a senso unico sicuro attraverso un firewall, alle applicazioni server in una rete non sicura.

Server Web. Un programma server che risponde alle richieste di risorse informative dai programmi browser.

Servizi di implementazione. L'installazione sul sito fornita dalla IBM

SOCKS, protocollo. Un protocollo che abilita un'applicazione in una rete sicura alle comunicazioni attraverso un firewall e un server socks.

spam. e-mail indesiderati, inviati spesso ad una infinità di destinatari.

SSL (Secure Sockets Layer). (1) Un protocollo di comunicazioni a standard IETF, che integra i servizi di sicurezza che sono il più trasparente possibile per l'utente finale. Fornisce un canale di comunicazione sicuro digitale. (2) Un server con capacità SSL accetta,

di solito, le richieste di collegamento SSL su una porta diversa da quella delle richieste HTTP normali. SSL crea una sessione durante la quale la procedura di handshake avviene solo una volta. Un volta terminata la procedura, le comunicazioni vengono cifrate. I controlli relativi all'integrità dei messaggi vengono eseguiti fino alla scadenza della sessione SSL.

T

TCP/IP. TCP/IP (Transmission Control Protocol/Internet Protocol).

TCP/IP (Transmission Control Protocol/Internet Protocol). Una serie di protocolli di comunicazione che supportano le funzioni di connettività peer-to-peer per le reti locali e per quelle ad ampia area.

telnet. Nell'insieme di protocolli Internet, telnet è un protocollo che fornisce il servizio di collegamento ad un terminale remoto. Consente agli utenti di un host di collegarsi ad un host remoto e di interagire come per gli utenti dei terminali ad esso collegati.

Token SecurID. Il metodo di autenticazione ACE/Server della Security Dynamics comprende un ID utente ed un token SecurID. Quando ci si collega in remoto, si ottiene la password dal token SecurID. La password cambia ogni 60 secondi ed è valida solo una volta. Anche se qualcuno riesce ad intercettare la password su una rete aperta, la password non è valida per ulteriori utilizzi.

traccia di analisi. I dati, in formato di percorso logico, che collegano una sequenza di eventi. Una traccia di analisi può essere utilizzata per eseguire la traccia di transazioni o la cronologia di una determinata attività. Ad esempio, può essere in grado di tenere traccia delle attività di un conto di un cliente.

U

URL. URL (Universal Resource Locator).

URL (Universal Resource Locator). La convenzione di denominazione utilizzata per le comunicazioni in Internet, in cui il percorso di un oggetto Web inizia con il nome servizio seguito da il nome dell'organizzazione, il percorso ed il nome file, ad esempio, http://www.ibm.com/software/security/firstsecure.

V

vault. Una vault utilizza la cifratura per proteggere le informazioni contro persone non autorizzate, come ad esempio i responsabili di sistema ed i proprietari di altre vault. Utilizza inoltre la firma digitale per proteggere da intrusioni ed la certificazione digitale per la protezione da comunicazione con sconosciuti. Utilizza inoltre la cifratura, la firma e la certificazione per trasmettere informazioni, in modo sicuro, ad altre vault.

VPN. VPN (Virtual Private Network).

VPN (virtual private network). Una rete di dati privata che utilizza Internet invece delle linee telefoniche per stabilire i collegamenti remoti. Siccome gli utenti accedono alle risorse aziendali di rete mediante un ISP (Internet Service Provider) invece di utilizzare un telefono aziendale, le organizzazioni riescono a ridurre in modo significativo, i costi degli accessi remoti. Una VPN migliora, inoltre, la sicurezza dello scambio di dati. Nella tecnologia firewall convenzionale, il contenuto dei messaggi può essere decodificato, mentre gli indirizzi di origine e destinazione non possono essere decodificati. Nella tecnologia VPN, gli utenti possono stabilire una connessione tunnel nella quale l'intero pacchetto di informazioni (contenuto ed intestazione), viene cifrato ed incapsulato.

W

wizard. Una casella di dialogo in una applicazione che utilizza le istruzioni passo-passo per guidare un utente nell'esecuzione di una specifica attività.

worm. Un virus dei computer che può essere pericoloso.

X

X.509. Uno standard per i certificati accettato quasi dappertutto, progettato per supportare le gestione sicura e la distribuzione di certificati PKI firmati digitalmente, nelle reti sicure Internet. Il certificato X.509 definisce le strutture dei dati che contengono procedure relative alla distribuzione di chiavi pubbliche firmate digitalmente da terze parti convalidate.

Indice analitico

G

H

I

J

S

T

U

V

W

X

Riservato ai commenti del lettore

IBM SecureWay FirstSecure
Pianificazione e integrazione
Versione 2 **CT7EHIT**

Commenti relativi alla pubblicazione in oggetto potranno contribuire a migliorarla.
Si invita il lettore ad usare lo spazio sottostante citando, ove possibile, i riferimenti alla pagina ed al paragrafo; i suggerimenti ed i commenti inviati potranno essere usati liberamente dall'IBM e dalla Selfin e diventeranno proprietà esclusiva delle stesse.
Si prega di non utilizzare questo foglio per richiedere informazioni tecniche su sistemi, programmi o pubblicazioni; per tali esigenze si consiglia di rivolgersi al punto di vendita o alla filiale IBM interessata.

Commenti:

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

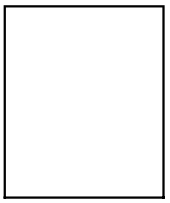
. . . . . .

Nome . . . . . .

Mansione/Titolo . . . . . .

Indirizzo . . . . . .

. . . . . Piegare . . . . . Piegare . . . . . .



SELFIN S.p.A.

Translation Assurance

via F. Giordani, 7

80122 - N A P O L I

Numero parte: CT7EHIT

Printed in Ireland