

Microsoft®

Internet Security & Acceleration Server 2006



ISA Server 2006 assicura protezione integrata, efficienza di gestione, velocità e protezione dell'accesso per qualsiasi tipo di rete.

Microsoft® Internet Security and Acceleration Server (ISA) 2006 è un gateway di protezione integrato che contribuisce a proteggere l'ambiente IT dalle minacce di Internet e offre agli utenti un accesso remoto veloce e sicuro a dati e applicazioni. ISA Server 2006 è disponibile in due edizioni: Standard ed Enterprise.

ISA Server 2006 è un'avanzata soluzione firewall con funzionalità stateful inspection di pacchetti e applicazioni, VPN (Virtual Private Network) e caching Web, che permette ai clienti di ottimizzare gli ambienti IT esistenti. ISA Server 2006 è una soluzione altamente protetta, conveniente e di facile utilizzo che consente ai professionisti IT di fronteggiare le nuove minacce che minano la sicurezza delle organizzazioni presenti in Internet.

ISA Server 2006 è il gateway di protezione integrato che offre:

Protezione integrata ISA Server 2006 protegge l'ambiente, i partner e gli utenti da programmi dannosi. La protezione è resa più efficace dall'integrazione con l'infrastruttura applicativa Microsoft e i servizi Microsoft Windows®, come l'autenticazione Kerberos e NTLM, il servizio Active Directory®, VPN, Routing e Accesso remoto, NLB (Network Load Balancing) e altri ancora. ISA Server 2006 è basato sulla piattaforma Windows Server™ 2003, che presenta meno vulnerabilità di qualsiasi sistema operativo Linux.

Gestione efficiente ISA Server 2006 semplifica l'implementazione di nuovi scenari di utilizzo con l'infrastruttura esistente, riducendo il TCO (Total Cost of Ownership) e semplificando la distribuzione e la gestione grazie a un'interfaccia di facile utilizzo, avanzati strumenti, un flessibile Software Development Kit (SDK), gestione remota e potenti funzionalità di registrazione e reporting.

Accesso veloce e sicuro ISA Server 2006 assicura la protezione di dati e applicazioni e la produttività degli utenti. Grazie alla compressione, alla cache, alle caratteristiche Single Sign-On e alle funzionalità di conversione dei collegamenti, ISA Server 2006 offre agli utenti un accesso veloce, semplice e sicuro alle applicazioni e ai dati aziendali.

Scenari di utilizzo

ISA Server 2006 si rivela di grande utilità per i responsabili IT, gli amministratori di rete e i responsabili della protezione delle informazioni che desiderano un livello superiore di sicurezza, prestazioni, gestibilità o una riduzione dei costi operativi delle reti. ISA Server 2006 permette di:

- **Pubblicare in modo sicuro contenuti accessibili in remoto**
ISA Server 2006 consente di ottimizzare le implementazioni aumentando la protezione delle applicazioni aziendali accessibili via Internet.
- **Connettere e proteggere le filiali dell'organizzazione**
ISA Server 2006 offre un'efficiente soluzione per espandere le reti aziendali in modo protetto, riducendo i costi delle reti grazie al migliore utilizzo delle connessioni esistenti.
- **Difendere l'ambiente dalle minacce esterne e interne basate sul Web**
ISA Server 2006 è stato progettato per consentire di gestire e proteggere le reti in modo più sicuro.

Pubblicare in modo sicuro contenuti accessibili in remoto

Le aziende devono consentire a dipendenti e partner di accedere in modalità remota ad applicazioni, documenti e dati da qualsiasi PC o dispositivo. La pubblicazione protetta delle applicazioni con ISA Server 2006 consente alle organizzazioni di rendere accessibili in modo più sicuro i propri server Exchange, SharePoint® e le applicazioni Web agli utenti remoti all'esterno della rete aziendale. Grazie alla pre-autenticazione degli utenti

prima che possano accedere a qualsiasi server pubblicato, alle funzionalità di stateful inspection anche per il traffico crittografato a livello di applicazione e a strumenti di pubblicazione automatizzati, ISA Server 2006 rende molto semplice aumentare la protezione delle applicazioni aziendali accessibili via Internet.

Connettere e proteggere le filiali dell'organizzazione

Le aziende devono assicurare la connessione delle filiali remote alla sede centrale, garantire un accesso protetto via Internet alle risorse aziendali e consentire di utilizzare al meglio le connessioni con una larghezza di banda limitata. Le organizzazioni possono utilizzare ISA Server 2006 come gateway per la connessione protetta delle filiali, utilizzando in modo efficiente la larghezza di banda della rete. Grazie a funzionalità come la compressione HTTP, il caching dei contenuti (inclusi gli aggiornamenti del software) e le funzionalità VPN integrate con filtro a livello di applicazione, ISA Server 2006 offre una soluzione conveniente per espandere e gestire in modo sicuro le reti aziendali.

Difendere l'ambiente dalle minacce esterne e interne basate sul Web

Le aziende devono eliminare gli effetti dannosi del malware e degli attacchi alla protezione tramite un set completo di strumenti per rilevare e bloccare contenuti, file e siti Web pericolosi. Le funzionalità di protezione dell'accesso al Web offerte da ISA Server 2006 possono aiutare le organizzazioni a proteggere il proprio ambiente dalle minacce interne ed esterne basate su Internet. Con un'architettura ibrida proxy-firewall, efficienti controlli dei contenuti, dettagliati criteri e avanzate funzionalità di monitoraggio e invio di avvisi, ISA Server 2006 rende più semplice gestire e proteggere le reti.

Publicare in modo sicuro contenuti accessibili in remoto

Protezione integrata	
Esigenza di aumentare la protezione e di utilizzare meglio l'autenticazione Active Directory, tenendo conto dei diversi dispositivi utilizzati per l'accesso.	Maggiore protezione e flessibilità di distribuzione per i server di applicazioni Web, grazie all' autenticazione multipla avanzata (smart card e password unica) , all'integrazione flessibile con Active Directory (LDAP) e all' autenticazione basata su moduli personalizzabili utilizzabili in quasi tutte le applicazioni Web e i dispositivi client.
Esigenza di metodi di autenticazione più avanzati per i server. Gli utenti mobili si connettono e abbandonano la sessione senza disconnettersi.	Facilità di integrazione con l'infrastruttura di autenticazione esistente grazie ai miglioramenti per la delega dell'autenticazione (inclusi NTLM, Kerberos e SecurID) e miglior controllo dell'accesso attraverso la gestione delle sessioni più efficiente , che rileva il traffico non generato dagli utenti tramite timeout automatici in base all'inattività.
Esigenza di protezione da attacchi mascherati come contenuto crittografato.	Utilizzo del bridging SSL (Secure Sockets Layer) per l'ispezione del contenuto crittografato, una maggiore scalabilità delle applicazioni (grazie al dirottamento del carico di lavoro dell'elaborazione SSL su ISA Server) e una latenza minore grazie al supporto per gli acceleratori hardware SSL.
Gestione efficiente	
Esigenza di pubblicare numerosi server Web e di applicazioni per soddisfare i crescenti requisiti di accesso remoto.	Semplicità di deployment di intere farm di server Web protette da ISA Server grazie alla funzionalità Web Publishing Load Balancing , che utilizza l'affinità in base alla sessione e all'indirizzo IP con rilevamento automatico dei malfunzionamenti.
La configurazione delle impostazioni per la pubblicazione dei server è problematica. Spesso durante la configurazione di SSL non è possibile sapere se i certificati sono validi.	Strumenti automatizzati per la pubblicazione protetta di Exchange, SharePoint e altri server Web , che semplificano il processo di pubblicazione di più siti, e amministrazione migliorata dei certificati per evitare errori di configurazione.
Esigenza di maggiore visibilità sulle risorse a cui accedono gli utenti e sulle modalità di accesso.	Efficienti funzionalità di registrazione e reporting consentono un monitoraggio avanzato dei client che accedono alle risorse aziendali, agevolando l'identificazione degli attacchi.
Accesso rapido e protetto	
Gli utenti remoti non possono accedere ai siti interni utilizzando i collegamenti nei messaggi di posta elettronica e devono autenticarsi più volte per accedere alle varie risorse aziendali.	Maggiore facilità di accesso alle applicazioni Web, alle raccolte di documenti e ai contenuti pubblicati grazie alla procedura Single Sign-On e alla conversione automatica dei collegamenti , che rendono più uniforme e sicura l'esperienza utente.

Connettere e proteggere le filiali dell'organizzazione

Protezione integrata	
I computer delle filiali non ricevono gli aggiornamenti del software con la rapidità necessaria.	Caching BITS per accelerare la distribuzione degli aggiornamenti del software e mantenere protetti i computer remoti.
Gestione efficiente	
Difficoltà di deployment nelle filiali remote perché non è disponibile personale IT locale per la configurazione di firewall o VPN.	Maggiore facilità di configurazione e deployment nelle filiali grazie a strumenti automatizzati per la connettività VPN e installazioni automatiche basate su file di risposte memorizzati su supporti rimovibili .
Esigenza di gestire in modo centralizzato la connettività e la protezione delle filiali e di evitare tempi di inattività della rete.	Gestione remota protetta di servizi firewall e di cache Web.
Esigenza di eseguire il deployment in ambienti IT esistenti senza modificare l'architettura di rete.	L'architettura a più reti, i modelli di rete e gli strumenti di configurazione rendono molto semplice e flessibile l'integrazione nell'infrastruttura esistente.
Accesso rapido e protetto	
I collegamenti WAN (Wide Area Network) sono costosi e poco utilizzati.	Caching e compressione del traffico HTTP per migliorare i tempi di caricamento delle pagine Web e ridurre i costi associati alle reti WAN per gli utenti nelle filiali remote.
Il traffico a bassa priorità può avere la precedenza su quello delle applicazioni business-critical nei collegamenti WAN, riducendo le funzionalità delle applicazioni.	Impostazioni IP di DiffServ per garantire che le applicazioni ad alta priorità abbiano la precedenza rispetto al resto del traffico di rete, migliorando l'utilizzo della larghezza di banda e i tempi di risposta per le risorse Web critiche.
Esigenza di migliorare le prestazioni della rete e di ottimizzare la distribuzione dei contenuti nelle filiali.	Funzionalità integrate di caching Web nei data center aziendali, array di server di cache e caching gerarchico distribuito .

Difendere l'ambiente dalle minacce esterne e interne basate sul Web

Protezione integrata	
Esigenza di contrastare un numero crescente di attacchi nelle risorse connesse al Web.	Funzionalità Enhanced Flood Resiliency per il monitoraggio e la gestione degli eventi, che offrono una maggiore resistenza agli attacchi Denial of Service e Distributed Denial of Service.
I worm che si propagano da un utente all'altro e da una rete all'altra danneggiano utenti, partner e clienti.	Riduzione degli effetti sulla rete dei computer colpiti da worm grazie al pooling degli avvisi IP e alle quote di connessione dei client.
Gli attacchi passano inosservati per ore o anche per giorni. Sono necessari mezzi migliori per rilevare gli attacchi in corso e porvi rimedio.	Funzionalità automatizzate per l'invio di avvisi e risposte permettono agli amministratori di ricevere velocemente notifiche in caso di attacchi o problemi della rete.
Gestione efficiente	
Esigenza di trovare velocemente le informazioni necessarie in caso di attacchi.	Maggiore controllo delle risorse grazie alla limitazione della registrazione nei log e al controllo dell'utilizzo della memoria e delle query DNS (Domain Name System) in sospenso.
Esigenza di controllo e reporting più dettagliati per numerosi gateway distribuiti nell'organizzazione.	Unificazione della gestione e del monitoraggio grazie al Management Pack di Microsoft Operations Manager 2005 e criteri a livello di azienda e di array che consentono agli amministratori di controllare facilmente le regole di protezione e di accesso in tutta l'organizzazione.
Accesso rapido e protetto	
Esigenza di proteggere le risorse IT e la proprietà intellettuale dell'azienda da attacchi e malware che sfruttano le attività degli utenti sul Web.	Il controllo a più livelli dei contenuti, i criteri completi e flessibili, i filtri personalizzabili per i protocolli e le relazioni di routing tra le reti assicurano la protezione dalle minacce basate su Internet.



© 2006 Microsoft. Tutti i diritti riservati.

Informiamo i gentili Clienti che i contenuti di questo documento hanno una valenza meramente indicativa, senza pretesa d'eshaustività o assenza di imprecisioni. Preghiamo i Clienti pertanto di farne oggetto d'attenta verifica e analisi.

Microsoft, Active Directory, SharePoint, Windows e Windows Server sono marchi o marchi registrati di Microsoft.

Altri nomi di prodotti e società citati nel presente documento possono essere marchi dei rispettivi proprietari.

Microsoft - Centro Direzionale S. Felice - Pal. A - Via Rivoltana, 13 - 20090 Segrate (MI)

Visitateci su Internet www.microsoft.com/italy/

Servizio Clienti 02.70.398.398, e-mail infoita@microsoft.com