

- Stateful Inspection von VPN-Verbindungen und Integration von VPN-Quarantänefunktionen bietet marktführende Sicherheit für VPN-Clients und Gateways. Auf den gesamten VPN-Datenstrom können die gleichen Regeln angewandt werden wie bei allen anderen Clients innerhalb des Netzwerks. Standards wie NAT-Traversal und der IPSec Tunnel Modus bieten darüber hinaus marktführende Technologie und Interoperabilität.
- Mit Hilfe der integrierten Multi-Networking-Funktionen sowie flexiblen Routing- oder NAT-Konfigurationen können Sie ISA Server 2004 in vorhandenen IT-Umgebungen als Haupt-, Abteilungs-, Zweigstellen- oder interne Firewall einsetzen, ohne die Netzwerkarchitektur ändern zu müssen.



Integrierte Unterstützung für Microsoft Exchange Server

ISA 2004 ermöglicht die sichere Veröffentlichung von Exchange Server-Postfächern mit Microsoft Outlook Web Access (OWA) oder Microsoft Outlook:

- Durch die HTTP-Filterung auch bei OWA SSL-Datenverkehr (SSL Bridging) können E-Mail-Inhalte schon an der Firewall eingehend auf gefährlichen Code hin überprüft werden.

- Eine vordefinierte Webveröffentlichungsregel ermöglicht sichere, formularbasierte Authentifizierung für OWA direkt auf der ISA 2004 Firewall.
- Durch Vorauthentifizierung am ISA Server 2004 werden anonyme Zugriffsversuche oder Denial-of-Service-Angriffe auf den OWA Server verhindert.
- Gleichzeitig ermöglicht Multifaktor-Authentifizierung stärkere Authentifizierungsmöglichkeiten über RADIUS (Remote Authentication Dial-In User Service) und Smart Cards, RSA SecurID.
- Mit Hilfe der Sitzungs-Time-outs wird verhindert, dass E-Mail-Sitzungen von Benutzern für unbegrenzte Zeit geöffnet bleiben.
- Der SMTP Message Screener ermöglicht Perimeter-basierte Abwehr von SPAM und Viren basierend auf Schlüsselwörtern und E-Mail-Anlagen.

Einfache Bedienung und wenig Komplexität

Die vollständig überarbeitete Benutzeroberfläche und die vereinfachten Verwaltungstools ermöglichen eine intuitive, einheitliche und wenig komplexe Firewall-, VPN- und Cache-Verwaltung. Der visuelle Richtlinien-Editor, Netzwerkvorlagen, Konfigurationsassistenten und verbesserte Problemdiagnosetools vermeiden Konfigurationsfehler und bieten dadurch mehr Sicherheit, unter anderem durch:

- Kurze Einarbeitungsphasen für neue Sicherheitsadministratoren.
- Umfassendes, didaktisch aufbereitetes Hilfesystem.
- Ein Firewall-Regelwerk, welches mit einem Blick erfasst werden kann.
- Administration auch über die Fernverwaltungskonsole oder eine Terminalverbindung.

- Volle Skriptfähigkeit der ISA 2004 Sicherheitsobjekte.
- Spezielle ISA 2004 Appliances von Microsoft Hardwarepartnern.



Schneller Zugriff auf Informationen

Mit ISA Server 2004 haben die Benutzer Ihres Unternehmens einen überaus schnellen, kosteneffizienten und gleichzeitig sicheren Zugriff auf die erforderlichen Informationen in Ihrem Netzwerk oder im Internet. Konkret bietet ISA Server:

- Standortunabhängigkeit beim Zugriff auf Unternehmensanwendungen und -daten, wie z. B. Microsoft Exchange Server oder die in Unternehmensportalen gespeicherten CRM-Daten.
- Single Sign-on für eine bequeme Einmalanmeldung mit standardkonformen Authentifizierungsmethoden.
- Erhöhte Netzwerkleistung und reduzierte Bandbreitenkosten durch Webcaching.
- Vordefinierte Serverrollen, bei denen nur die wirklich benötigten Dienste – wie z. B. für die Unternehmens-Firewall, die VPN-Lösung oder einen Webcache – in kurzer Zeit bereitgestellt werden können.

Vorteile und Einsatzszenarien für Unternehmen jeder Größe

Als integrierte Firewall-, VPN- und Caching-Lösung bietet ISA Server 2004 gerade kleinen und mittleren Unternehmen die Möglichkeit, ihre Investitionen in Microsoft-Technologien optimal zu nutzen. Mit ISA Server können Sie Ihre Sicherheits- und Unternehmensanforderungen auf kosteneffiziente Weise erfüllen und zusätzliche Produktivität für Ihre Mitarbeiter erreichen.

Große Unternehmen haben die Möglichkeit, mit ISA Server 2004 ihre Investitionen in Microsoft-Technologien zu schützen und auszubauen. ISA Server 2004 ist für die Anbindung von Niederlassungen optimal geeignet. Durch eine zentrale Verwaltung von Firewall-Sicherheitsrichtlinien können Unternehmen ihr Sicherheitskonzept konsolidieren und Kosten senken. ISA Server 2004 bietet unter anderem folgende Einsatzszenarien:

- Die Mitarbeiter-Desktops und Unternehmensserver werden vor gefährlichem Datenverkehr geschützt.
- Die Internetnutzung der Mitarbeiter im Internet kann kontrolliert und gefiltert werden.
- Remote Access VPNs für Mitarbeiter und Geschäftspartner auf ausgewählte Bereiche des Unternehmensnetzwerks.
- Zweigstellen können mit der Zentrale sowie untereinander durch Site-to-Site VPNs verbunden werden.
- Die Netzwerkleistung kann durch Webcaching enorm gesteigert werden.

Produkt-Highlights

Feature	Vorteil
Wichtige Unternehmensanwendungen und -daten schützen	
Inhaltsüberprüfung in allen Schichten des Datenverkehrs	Mit einer technisch ausgereiften Firewall werden IT-Umgebungen vor Schad-Code und Crackern geschützt, indem unerwünschter Datenverkehr bis in die Anwendungsebene der Protokolle untersucht wird.
Optimale Abstimmung auf unterschiedlichste Anwendungen	Benutzer profitieren von einem schnelleren, sicheren Zugriff auf Anwendungen und Dienste wie Microsoft Exchange Server, Microsoft-Internet-Information Services (IIS) und Web-Portale.
Integrierte VPN-Funktionen mit VPN-Filterung	Problemlose Konfiguration von Remote Access VPNs oder Site-to-Site VPNs ermöglichen für Mitarbeiter und Partner sichere Netzwerkanbindung und mehr Produktivität. Unterstützung für alle VPN-Standardprotokolle inklusive IPSec-Tunnelmodus gewährleistet weitreichende Interoperabilität.
Vielseitige Authentifizierungsmechanismen	Benutzer werden an der Firewall über integrierte Windows- oder RADIUS-Namensräume identifiziert. Starke Authentifizierungsmechanismen wie Smart Cards oder RSA SecurID Tokens werden unterstützt.
Netzwerksicherheitsrichtlinien und Firewall-Konfiguration problemlos verwalten	
Multi-Networking-Funktionen und -Vorlagen	ISA Server 2004 integriert sich problemlos in bestehende IT-Umgebungen als Grenz-, Zweigstellen-, Abteilungs- oder innere Firewall zur Segmentierung des Netzwerks. Netzwerkvorlagen helfen bei der sicheren Konfiguration und bilden die Basis für netzwerkspezifische Firewall-Richtlinien.
Einfache Verwaltungsoberfläche für Firewall, VPN und Cache	Besonders benutzerfreundliche Verwaltungstools, wie der visuelle Firewall-Richtlinien-Editor, helfen, die Inbetriebnahme zu beschleunigen und fehlerhafte Konfigurationen zu vermeiden.
Status optimal im Griff	Das neue Monitoring-Dashboard mit Echtzeit-Protokollierungsanzeige ermöglicht den schnellen Abruf von Überblick- oder Detaildaten zum Firewall-Status wie aktueller Datendurchsatz, Sitzungen und Alarme.
Zugriff beschleunigen und Effizienz steigern	
Verbesserte Firewall-Architektur	Autorisierter Datenverkehr kann die Firewall auch bei Filterung auf Anwendungsebene sehr schnell durchlaufen. Durch die Kernelmodus-Datapump werden Netzwerkeffizienz und Produktivität erhöht.
Schnellerer, kostengünstigerer Internetzugriff	Durch den integrierten ISA Server-Webcache (unterstützt Forward- und Reverse-Caching) für die schnellere Bereitstellung von Inhalten werden Benutzerproduktivität gesteigert und Bandbreitenkosten gespart.

8% \$"
!
4% # 7#
'% ' 4
A , / # 4
< % % 4
-
!!" #

Sicherheitsinfrastruktur

Verbessert	Anwendungsfilterung	Mit ISA Server 2004 können Sie aus einer Vielzahl von neuen Funktionen für die Anwendungsfilterung und Serververöffentlichung wählen. Zu den neuen Filterfunktionen gehört die verbesserte HTTP-Filterung. Sie ist speziell für Exchange Server, Outlook Web Access und Internet Information Server ausgelegt.
Neu	Umfassende Unterstützung von Protokollen	Dank zahlreicher vordefinierter Protokolle können Sie ISA Server 2004 in gängige Internetanwendungen integrieren. ISA Server 2004 ermöglicht die Kontrolle des Zugriffs auf jedes Protokoll sowie deren Nutzung. Dazu gehören IP-Protokolle und IPSec-Datenverkehr.
Verbessert	Authentifizierungsmechanismen	Die Benutzer können mit Hilfe integrierter Windows-, RADIUS- oder RSA SecurID-Authentifizierungstypen oder -Namensräume authentifiziert werden. Dabei werden Regeln für Benutzer oder Benutzergruppen in jedem Namensräume angewendet.
Verbessert	Vereinfachtes Richtlinienmodell	ISA Server 2004 verwendet jetzt ein einheitlich aufgebautes Regelmodul mit detaillierten Mechanismen für die Verwaltung von Datenverkehr und das Erzwingen von Richtlinien. Mit Hilfe dieses Regelmoduls können Administratoren den Netzwerk- und Internetzugriff nach Benutzern, Gruppen, Anwendungen, Inhalt, Zeitplan und Ziel kontrollieren.
	Dynamische Paketfilterung	ISA Server 2004 verringert das Risiko externer Angriffe, indem Ports nur bei Bedarf geöffnet werden.
Verbessert	Aktualisierter Firewall-Client	Der ISA Server 2004-Firewall-Client ermöglicht Ihnen die Integration von Authentifizierungsmethoden, der automatischen Webproxy-Konfiguration und der rollenbasierten Sicherheit mit Hilfe von Gruppenrichtlinien. Die bessere Konnektivität für komplexe Protokolle, die Unterstützung von Konten für mehrere Benutzer und die verschlüsselte Kommunikation sind weitere wichtige Verbesserungen.
	Transparenz für alle Clients	ISA Server 2004 ist mit Clients und Anwendungsservern – darunter auch NAT- und SecureNAT-Clients – auf allen Plattformen kompatibel, ohne dass hierfür Client-Software benötigt wird.
Verbessert	Veröffentlichung	Mit ISA Server 2004 können Sie Server im Unternehmensnetzwerk oder in einem Umkreisnetzwerk hinter der Firewall platzieren und die hierauf ausgeführten Dienste sicher im Internet veröffentlichen.
	Link-Übersetzung	Die Link-Übersetzungsfunktion in ISA Server 2004 ermöglicht eine intelligente Übersetzung von internen Links in öffentlich zugängliche Websites.

Webcache

Verbessert	Cache-Regeln	Über einen zentralen Mechanismus für Cache-Richtlinien können Sie genau festlegen, wie im Cache gespeicherte Objekte abgerufen und bereitgestellt werden.
	Effiziente Verteilung von Inhalten	Durch die Zwischenspeicherung von Websites und E-Commerce-Anwendungen können Sie die Antwortzeiten verkürzen und die Bandbreitenkosten senken.
	Hochleistungsfähiger Webcache	Durch das Webcaching werden der Webzugriff beschleunigt und Einsparungen bei der Netzwerkbandbreite ermöglicht.
	Optimale Zwischenspeicherung	Sie können häufig benötigte Objekte proaktiv zwischenspeichern, um jedem Benutzer aktuelle Inhalte zur Verfügung zu stellen. Sie können auch ganze Websites nach einem festen Zeitplan in den Zwischenspeicher laden.

Verwaltung

Verbessert	Verwaltung	Mit den neuen Verwaltungs-Features ist es jetzt noch einfacher, Netzwerke zu schützen. ISA Server 2004 bietet zudem neue Features wie Aufgabenbereiche, Hilfebereiche und einen neu gestalteten Firewall Richtlinien-Editor mit Drag & Drop-Funktionen.
Neu	Export und Import	Mit ISA Server 2004 ist es jetzt möglich, Konfigurationsdaten zwischen ISA Server-Computern über eine XML-Datei zu exportieren und zu importieren. So können Sie Firewall-Konfigurationen bei einer Bereitstellung an mehreren Standorten problemlos replizieren.
Neu	Übersicht („Dashboard“)	In einer zentralen Statusübersicht wird eine Zusammenfassung aller wichtigen Überwachungsinformationen angezeigt. Wenn Sie ein Problem entdecken, können Sie einfach Detailinformationen abrufen.
Neu	Protokollanzeige	Über die Protokollanzeige können Sie die Firewall-Protokolle in einem Echtzeit-Onlinemodus oder als zeitlichen Verlauf anzeigen. Durch Filterung können spezifische Einträge sehr schnell gefunden werden.
Verbessert	Integrierte Berichterstellung	Sie können zeitgesteuert Standardberichte mit Informationen über Webnutzung, Anwendungsnutzung, Datenverkehr und Sicherheit erstellen.

Leistungsfähige Partner-Lösungen

ISA Server 2004 beinhaltet wie sein Vorgänger leistungsfähige Schnittstellen und ein Software Development Kit, um Sicherheits- und Verwaltungsfunktionen hinzuzufügen. Etliche Lösungen von Microsoft-Partnern bieten ergänzende Funktionalitäten für die Bereiche Application Layer Filtering, Content Security, High Availability und Load Balancing, Intrusion Detection, Reporting und mehr. Informationen zu diesen Lösungen finden Sie auf den ISA Server-Webseiten.

Voraussetzungen

Für die Verwendung von Microsoft Internet Security & Acceleration Server 2004 Standard Edition benötigen Sie Folgendes:

- Einen PC mit einem Pentium III-Prozessor mit 550 MHz oder höher (ISA Server 2004 Standard Edition unterstützt bis zu vier CPUs auf einem Server)
- Microsoft Windows® 2000 Server oder Advanced Server mit Service Pack 4 oder höher, Windows 2000 Datacenter Server oder Windows Server 2003 Standard Edition oder Enterprise Edition
- 256 MB RAM oder mehr (empfohlen)
- Eine lokale, NTFS-formatierte Partition mit 150 MB verfügbarem Festplattenspeicher; zusätzlicher Speicherplatz für Webcaching-Inhalte
- Einen mit dem Betriebssystem des Computers kompatiblen Netzwerkadapter für die Kommunikation mit dem internen Netzwerk; einen zusätzlichen Netzwerkadapter, ein Modem oder einen ISDN-Adapter für jedes weitere Netzwerk, das mit dem ISA Server-Computer verbunden wird

- CD-ROM- oder DVD-ROM-Laufwerk
- Monitor mit VGA- oder höherer Auflösung
- Tastatur und Microsoft Mouse oder kompatibles Zeigergerät

Anmerkungen:

Wenn Sie ISA Server 2004 Standard Edition unter Windows 2000 Server installieren, benötigen Sie Folgendes: Windows 2000 Service Pack 4 oder höher sowie Internet Explorer 6 oder höher. Wenn Sie die Versionen Windows 2000 Server oder Advanced Server mit Service Pack 4 verwenden, müssen Sie das im Microsoft Knowledge Base-Artikel 821887 angegebene Hotfix installieren.

Microsoft empfiehlt allen Kunden, die unter

www.microsoft.com/germany/ms/security/default.mspx

beschriebenen bewährten Methoden zur Erhöhung der Sicherheit anzuwenden. Möglicherweise sind zusätzliche Updates erforderlich. Die tatsächlichen Systemanforderungen sind abhängig von Ihrer Konfiguration, der erwarteten Auslastung und den von Ihnen installierten Features.

Weitere Informationen zu Microsoft Internet Security & Acceleration Server 2004, Whitepapers, Partner-Lösungen und Case-Studies finden Sie unter:

www.microsoft.com/germany/isa

© 2004 Microsoft Corporation. Alle Rechte vorbehalten.

Dieses Datenblatt dient nur zu Informationszwecken. MICROSOFT SCHLIESST FÜR DIESE ZUSAMMENFASSUNG JEDE GEWÄHRLEISTUNG AUS, SEI SIE AUSDRÜCKLICH ODER KONKLUDENT. Microsoft, Active Directory, Outlook, SharePoint, Windows und Windows Server System sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Die in diesem Dokument aufgeführten Namen tatsächlicher Firmen und Produkte können geschützte Marken ihrer jeweiligen Eigentümer sein.



Windows Server System ist eine übergreifende, integrierte Serverinfrastruktur. Diese erleichtert die Entwicklung, Installation und Anwendung flexibler Unternehmenslösungen.

www.microsoft.com/germany/windowsserversystem