

ISA Server 2004 – das Produkt im Überblick

Einleitung

Microsoft® Internet Security & Acceleration Server 2004 (ISA Server 2004) ist eine technisch ausgereifte Firewall-, VPN- und Webcachelösung auf Anwendungsebene, die durch verbesserte Netzwerksicherheit und Leistung die maximale Nutzung vorhandener IT-Bestände ermöglicht.

ISA Server 2004 besticht durch optimalen Datenschutz und einfache Bedienung sowie durch einen schnellen, sicheren Zugriff auf jede Art von Netzwerk. Das Produkt eignet sich insbesondere für den Schutz von Netzwerken, in denen Microsoft-Anwendungen ausgeführt werden, wie beispielsweise Outlook® Web Access, Microsoft Internet Information Server, Office SharePoint® Portal Server, Routing- und RAS-Server, der Verzeichnisdienst Active Directory®.

ISA Server 2004 ist eine vielseitig einsetzbare Firewall auf Anwendungsebene, mit der sich Unternehmen jeder Größe vor Angriffen von außen oder vor internen Bedrohungen schützen können. Mit ISA Server 2004 ist eine gründliche Prüfung von Internetprotokollen wie HTTP gewährleistet, sodass viele Angriffe abgewehrt werden können, die von herkömmlichen Firewalls nicht erkannt werden.

Die integrierte Firewall- und VPN-Architektur von ISA Server ermöglicht eine statusabhängige Filterung und Überprüfung des gesamten VPN-Verkehrs. Zudem können bei Microsoft Windows Server 2003-basierten Quarantänelösungen VPN-Clients überprüft werden, um Netzwerke vor Angriffen über eine VPN-Verbindung zu schützen.

Die neu gestaltete Benutzeroberfläche sowie die Assistenten, Vorlagen und zahlreiche Verwaltungstools helfen Administratoren dabei, gängige Fehler bei der Sicherheitskonfiguration zu vermeiden.

ISA Server 2004 – Einsatzmöglichkeiten

ISA Server bietet neue Möglichkeiten für IT-Manager, Netzwerkadministratoren und IT-Sicherheitsexperten, die für die Sicherheit, Leistung, Verwaltbarkeit oder Betriebskosten ihrer Netzwerke verantwortlich sind. ISA Server 2004 ist dabei für Unternehmen jeder Größe geeignet. In den folgenden Abschnitten werden einige Netzwerkszenarien beschrieben, in denen ISA Server 2004 zum Einsatz kommen kann.

Sichere E-Mail-Nutzung

Ermöglichen Sie Mitarbeitern außerhalb des Netzwerks den problemlosen Zugriff auf E-Mails – ohne Sicherheitsrisiko

ISA Server 2004 gewährleistet optimalen Schutz für OWA-Websites (Microsoft Outlook Web Access): Dank der unkomplizierten Verwaltungsoberfläche von ISA Server 2004 können Unternehmen ohne großen Aufwand eine Webveröffentlichungsregel einrichten, die eine sichere, formularbasierte Authentifizierung erzwingt.

ISA Server 2004 wehrt auch Angriffe auf E-Mail-Server ab: Dank der SSL-Verschlüsselung (Secure Sockets Layer) kann SSL-Datenverkehr nach gefährlichem Code durchsucht werden. Darüber hinaus ist durch die HTTP-Filterung eine gründliche Überprüfung von Anwendungsinhalten gewährleistet.

Durch die Vorauthentifizierung in ISA Server 2004 werden zudem anonyme Benutzeranmeldungen verhindert – eine wichtige Voraussetzung für den Schutz interner Server.

Mit einem komplexen Authentifizierungssystem kann überprüft werden, ob bei Remote-Mails RADIUS (Remote Authentication Dial-In User Service) oder RSA SecurID verwendet wird. So können Sie verhindern, dass anonyme Anfragen, von denen eine potenzielle Gefahr ausgeht, überhaupt den Microsoft Exchange Server erreichen.

Einen zusätzlichen Schutz bieten die Funktionen zur Blockierung von Anhängen sowie die Sitzungstimeouts. Sie verhindern, dass E-Mail-Sitzungen für unbegrenzte Zeit geöffnet bleiben und für andere Benutzer zugänglich sind.

Abbildung 1 zeigt, wie ISA Server 2004 die Sicherheit beim Zugriff auf E-Mails durch Mitarbeiter außerhalb des Unternehmensnetzwerks.

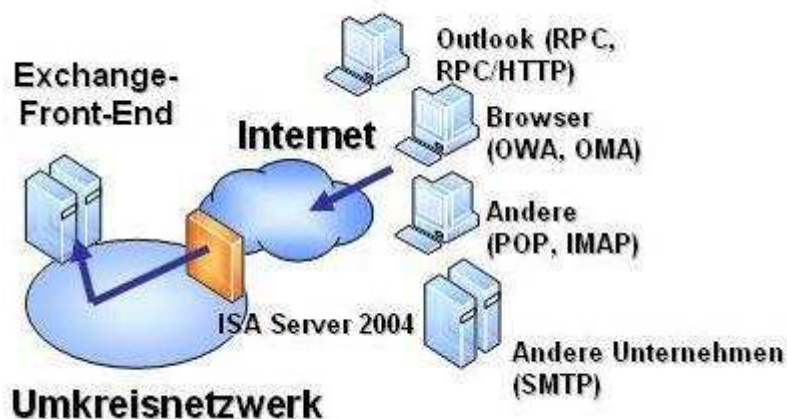


Abbildung 1: Mit ISA Server 2004 können Sie mühelos und ohne Sicherheitsrisiko Mitarbeitern außerhalb des Unternehmensnetzwerks den Zugriff auf E-Mails ermöglichen.

Sichere Veröffentlichung von Web-Servern

Stellen Sie Intranetinformatoren sicher und einfach im Internet bereit

Mit Hilfe der Web- und Serververöffentlichungsfunktionen von ISA Server 2004 können Intranetanwendungen Informationen sicher im Internet veröffentlichen. Mit den Assistenten für Web- und Serververöffentlichung werden häufige Aufgaben automatisiert und das Risiko fehlerhafter Konfiguration reduziert.

Die Linkübersetzungsfunktionen ermöglichen zudem eine optimale Umwandlung von Internetlinks in öffentlich zugängliche Websites. ISA Server 2004 kann auch die Gültigkeit von Datenverkehr überprüfen, die Verwendung gültiger URLs erzwingen und Benutzer über vorhandene Authentifizierungssysteme vorab authentifizieren. So können Sie verhindern, dass gefährliche anonyme Anfragen veröffentlichte Server erreichen.

Abbildung 2 zeigt, wie ISA Server 2004 bei der Bereitstellung von Intranetinformatoren über das Internet Ihr Unternehmensnetzwerk schützen kann.

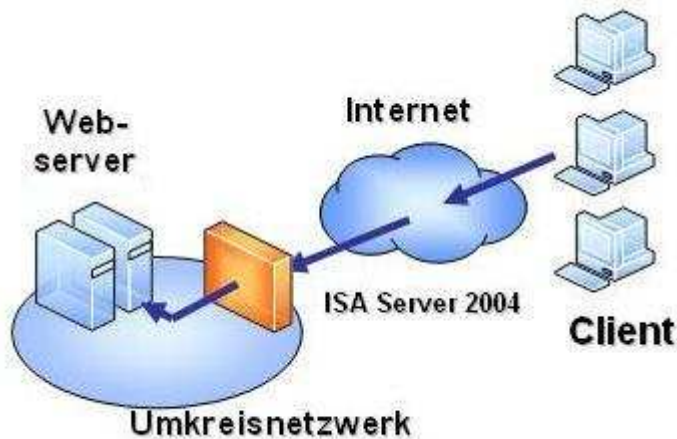


Abbildung 2: ISA Server 2004 ermöglicht eine sichere und einfache Veröffentlichung von Intranetinformationen im Internet.

Sichere Anbindung von Geschäftspartnern

Ermöglichen Sie Ihren Partnern den sicheren Zugriff auf relevante Informationen im Unternehmensnetzwerk

Mit Hilfe der integrierten VPN-Funktionen von ISA Server 2004 können Sie Ihren Geschäftspartnern den Zugang zu Ihrem Unternehmensnetzwerk ermöglichen, wobei Sie aber den Zugriff auf spezielle Server und Anwendungen beschränken können.

ISA Server 2004 verschlüsselt den gesamten Datenverkehr zwischen Ihrem Geschäftspartner und dem Unternehmensnetzwerk. So sind die Daten geschützt und können nicht geändert werden. VPN-Endpunktserver führen zudem untereinander Authentifizierungen durch. Nach einer Authentifizierung erzwingt ISA Server 2004 Zugriffs- und Routingrichtlinien, die den Zugriff des Partners auf das Unternehmensnetzwerk einschränken.

Sie können mit ISA Server 2004 auch strenge Anwendungsfiler-Regeln implementieren, um Ihr Unternehmensnetzwerk besser vor Angriffen auf Anwendungsebene zu schützen.

Abbildung 3 zeigt, wie Sie mit ISA Server Ihren Geschäftspartnern wichtige Informationen zur Verfügung stellen können, ohne das Unternehmensnetzwerk zu gefährden.

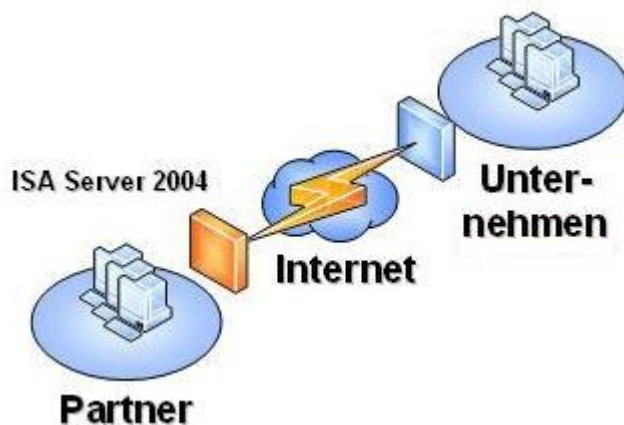


Abbildung 3: Mit ISA Server 2004 können Sie Ihren Geschäftspartnern einen sicheren Zugriff auf relevante Unternehmensinformationen bieten.

Sichere Remote-Verbindungen

Ermöglichen Sie Ihren Mitarbeitern einen sicheren und flexiblen Remotezugriff, und schützen Sie das Unternehmensnetzwerk vor gefährlichem Datenverkehr

Durch eine technisch ausgefeilte Filterung auf Anwendungsebene verhindert ISA Server 2004, dass nicht verwaltete Remotecomputer über ein VPN auf das Unternehmensnetzwerk zugreifen.

Der Datenverkehr wird überprüft und analysiert, um Computerwürmer und Viren abzufangen. Sie können ISA Server auch dazu nutzen, VPN-Benutzern- und -Gruppen flexible Netzwerkrichtlinien zuzuweisen, damit sie nur auf bestimmte Server und Anwendungen zugreifen.

Um die Sicherheit noch weiter zu erhöhen, kann ISA Server 2004 Clients isolieren (VPN Quarantäne), die vordefinierte Sicherheitsrichtlinien des Unternehmens hinsichtlich Installation von Softwareupdates, Antivirusprogrammen oder speziellen Computerkonfigurationen nicht erfüllen.

Abbildung 4 zeigt, wie ISA Server beim Remotezugriff durch Mitarbeiter das Unternehmensnetzwerk schützt.

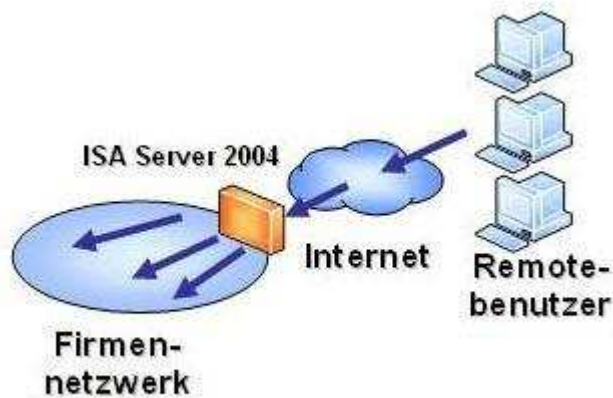


Abbildung 4: Mit ISA Server 2004 können Sie Mitarbeitern einen sicheren und flexiblen Remotezugriff auf das Unternehmensnetzwerk ermöglichen und dabei das Netzwerk vor gefährlichem Datenverkehr schützen.

Sichere Standort-Verbindungen

Sorgen Sie für eine sichere Internetkommunikation zwischen Ihren Zweigstellen und der Unternehmenszentrale

Mit Hilfe eines ISA Server 2004-VPN-Gateways kann ein Administrator ganze Netzwerke über Site-to-Site-Verbindungen miteinander verbinden – so auch die Zentrale eines Unternehmens mit den Zweigstellen.

Der IPSec-Tunnelmodus der VPN-Funktion von ISA Server 2004 ermöglicht es dem Firewall-Administrator strenge Zugriffssteuerungen für Datenverkehr über die Site-to-Site-Verbindung festzulegen. (z.B. Steuerungen auf Benutzer-, Gruppen-, Website-, Computer-, Protokoll- und Anwendungsebene)

Durch diese Kontrolle können Benutzer im lokalen Netzwerk nur auf bestimmte Inhalte im Remote-Netzwerk zugreifen, und Remotenetzwerk-Benutzer können nur auf jeweils freigegebene lokale Netzwerkressourcen zugreifen.

In Abbildung 5 können Sie sehen, wie ISA Server für sichere Verbindungen zwischen Zweigstellen und der Zentrale sorgt:

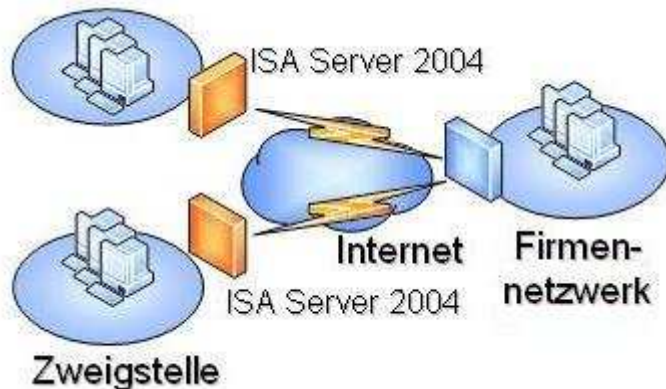


Abbildung 5: ISA Server garantiert sichere Verbindungen zwischen Zweigstellen und der Zentrale.

Sichere Internetnutzung

Kontrollieren Sie den Internetzugriff, und schützen Sie Clients vor gefährlichem Internetdatenverkehr

Mit ISA Server 2004 ist es sehr einfach, Internetzugriffs-Richtlinien für die Benutzer festzulegen und diese vor gefährlichen Internetdaten zu schützen. Flexible Firewall-Richtlinien ermöglichen die Blockierung von Websites sowie die Filterung von Inhalten.

So wird die Produktivität gesteigert und unerwünschte Inhalte werden blockiert. ISA Server ist zudem bestens auf Active Directory abgestimmt, sodass Sie für unterschiedliche Unternehmensrollen und -Funktionen benutzerdefinierte Zugriffssteuerungen einrichten können.

Die Filterung auf Anwendungsebene bietet eine höhere Zuverlässigkeit für Ihre Umgebung, da Desktops und Server auch vor besonders tückischen Angriffen geschützt sind. Durch die zuverlässige HTTP-Filterung in ISA Server 2004 kann z.B. die Verwendung von Peer-to-Peer- und Instant Messaging-Anwendungen unterbunden werden.

Die Filterung des Datenverkehr wehrt eine Vielzahl häufiger Angriffsformen ab, indem der externe Zugriff auf interne Clients unterbunden und die Gültigkeit eingehender Antwortdaten überprüft wird. Zudem werden von Drittanbietern Add-Ons zum Schutz vor Spam, Würmer und Viren bereits an der Firewall angeboten.

Abbildung 6 zeigt, wie ISA Server den Internetzugriff kontrolliert und Clients vor gefährlichen Internetdaten schützt.

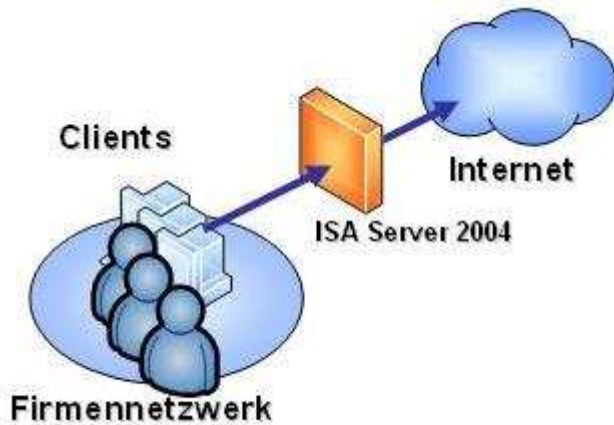


Abbildung 6: ISA Server 2004 kontrolliert den Internetverkehr und schützt Clients vor gefährlichem Datenverkehr.

Nutzung von Webinhalten mit hoher Performance

Sorgen Sie für einen schnellen Zugriff auf häufig genutzte Webinhalte

Die Cachingfunktionen von ISA Server 2004 garantieren einen schnellen Zugriff auf häufig benötigte Webinhalte. Mit Hilfe der Caching- und Abfangfunktionen werden Muster im Webdatenverkehr ermittelt und häufig aufgesuchte Websites automatisch gedownloadet, damit sie sofort abrufbar sind.

ISA Server kann zudem spezielle Anfragen an Upstream-Cachingserver weiterleiten, wenn der Downstreamcache voll ist.

Die Abbildungen machen deutlich, wie ISA Server mit Hilfe der Downstream- und Upstream-Cachingfunktionen einen schnellen Zugriff auf häufig benötigte Webinhalte ermöglicht:

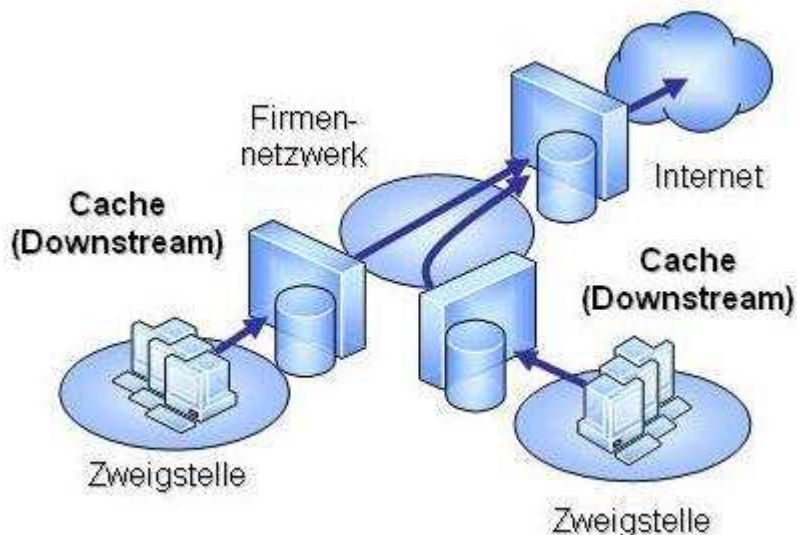


Abbildung 7: Durch Downstreamcaching sind häufig benötigte Webinhalte schnell abrufbar.

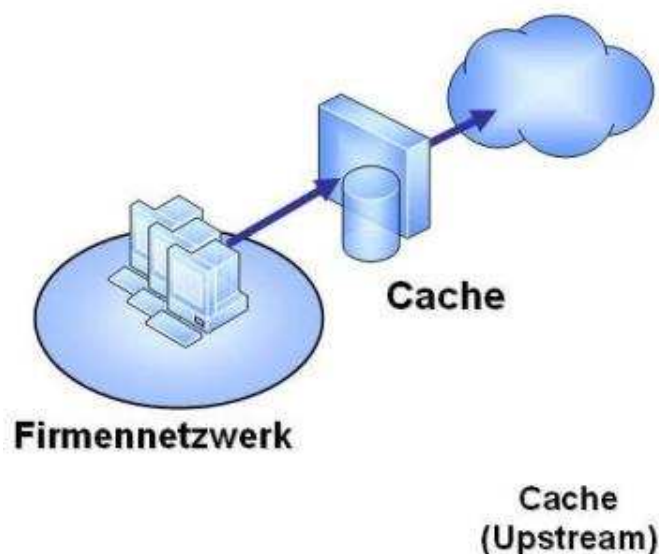


Abbildung 8: Upstreamcaching steht zur Verfügung, wenn Downstreamcaches voll sind.

Microsoft ISA Server — Die Features

Microsoft ISA Server 2004 zeichnet sich gegenüber anderen Firewalllösungen vor allem durch fortschrittliche Schutzfunktionen, unkomplizierte Bedienung und durch einen schnellen und sicheren Internetzugriff aus.

Optimaler Schutz

ISA Server 2004 ist darauf ausgelegt, durch statusabhängige Paketfilterung und Filterung auf Sitzungsebene Ihr Unternehmen vor neuartigen Angriffen zu schützen. Mit Hilfe der statusabhängigen Paketfilterung wird festgelegt, welche Pakete die gesicherte Netzwerksitzung und die Proxydienste auf Anwendungsebene erreichen dürfen.

Durch diese Filterung werden Ports nur bei Bedarf geöffnet und nach Beendigung der Kommunikation wieder geschlossen. Bei der Filterung auf Sitzungsebene stehen anwendungstransparente Gateways auf Sitzungsebene für einen Multiplattformzugriff auf Windows Media®-Technologien, Telnet, RealAudio, IRC und viele andere Internetprotokolle und Dienste zur Verfügung. Die Sicherheit auf Sitzungsebene und die dynamische Paketfilterung erhöhen die Sicherheit und den Benutzerkomfort.

Zusätzlich zur statusabhängigen Paketfilterung und zur Filterung auf Sitzungsebene kontrolliert ISA Server 2004 auch anwendungsspezifischen Datenverkehr mit Anwendungs-, Befehls- und Datenfiltern. Durch die intelligente Filterung von VPN-, HTTP-, FTP-, SMTP-, POP3-, DNS-, H.323-Conferencing-, Streaming Media- und RPC-Daten kann ISA Server Datenverkehr je nach Inhalt akzeptieren, ablehnen, weiterleiten oder ändern.

Benutzerfreundlichkeit

ISA Server 2004 zeichnet sich durch eine flexible und einfache Verwendung aus. Vor allem die Multi-Networkingarchitektur, die einheitliche VPN- und Firewallverwaltung über einen zuverlässigen visuellen Richtlinien-Editor, intuitiv nutzbare Netzwerkvorlagen, automatisierte Assistenten und verbesserte Problembehandlungstools tragen zu einer hohen Benutzerfreundlichkeit bei.

Zudem ist die Firewalleinrichtung dank der automatischen Installation von Firewall- und Webcachingkomponenten äußerst einfach. Darüber hinaus können z.B. Konfigurationsinformationen

in XML exportiert, Firewall Sitzungen in Echtzeit überwacht und Firewallbenutzergruppen im Active Directory genutzt werden.

Schneller und sicherer Zugriff

Durch die vollständige Integration von VPN-Funktionen in die Firewallarchitektur, das beschleunigte Webcaching und die hohe Geschwindigkeit bei der Firewallfilterung bietet ISA Server 2004 einen schnellen und sicheren Internetzugriff. Dank der integrierten Unterstützung des IPsec-Tunnelmodus für Site-to-Site-VPNs kann ISA Server 2004 problemlos mit den VPN-Anbietern der Niederlassungen verbunden werden. Durch die Unterstützung des IPsec-Tunnelmodus sind auch eine gründliche Überprüfung von VPN-Clients und eine Unterstützung von Firewallrichtlinien für Windows-basierte Quarantänelösungen gegeben. Auf diese Weise können die Benutzer eines Unternehmens deutlich sicherer arbeiten. Die Unterstützung moderner Filter von Drittanbietern und ein umfassendes Software Development Kit (SDK) runden das Angebot ab.

Die Features auf einen Blick

In Tabelle 1 werden die Hauptfeatures von ISA Server 2004 vorgestellt.

Tabelle 1. Microsoft ISA Server — Die Features auf einen Blick	
Feature	Beschreibung
Unternehmensfirewall für mehr Sicherheit	
Sicherheit durch Multilayer-Firewall	<p>Mit der Filterung von Datenverkehr auf Paket-, Sitzungs- und Anwendungsebene können Unternehmen für eine maximale Sicherheit sorgen.</p> <p>Durch eine statusabhängige Paketfilterung wird festgelegt, welche Pakete die gesicherte Netzwerksitzung und die Proxydienste auf Anwendungsebene erreichen dürfen. Durch diese Filterung werden Ports nur bei Bedarf geöffnet und nach Beendigung der Kommunikation wieder geschlossen.</p> <p>Bei der Filterung auf Sitzungsebene stehen anwendungstransparente Gateways auf Sitzungsebene für einen Multiplattformzugriff auf Telnet, RealAudio, Windows Media-Technologien, IRC und viele andere Internetprotokolle und Dienste. Anders als andere Proxys auf Sitzungsebene sind die ISA Server-Sicherheitsfunktionen auf Sitzungsebene mit der dynamischen Paketfilterung für eine höhere Sicherheit und Benutzerfreundlichkeit kombinierbar.</p> <p>Bei der Anwendungsfilterung und statusabhängigen Prüfung (Stateful Inspection) werden Befehle in den Anwendungsprotokollen der Clientcomputer (wie z.B. HTTP, FTP und Gopher) verstanden. ISA Server agiert auf Seiten des Clientcomputers. Die Netzwerktopologie und IP-Adressen sind für das externe Netzwerk nicht einsehbar.</p>
Statusabhängige Prüfung	ISA Server 2004 führt an der Firewall eine dynamische statusabhängige Prüfung von Datenverkehr auf Anwendungsebene durch. Um einen sicheren Datenschutz zu gewährleisten und Sicherheitsverletzungen zu verhindern, erfolgt die Überprüfung im Kontext des Protokolls auf Anwendungsebene und des Verbindungsstatus.
Intelligente Anwendungsfilterung	ISA Server 2004 bietet mehr als eine übliche Anwendungsfilterung: Anwendungsspezifischer Datenverkehr wird mit Anwendungs-, Befehls- und Datenfiltern kontrolliert. Durch die intelligente Filterung von VPN-, HTTP-, FTP-, SMTP-, POP3-, DNS-, H.323-Conferencing-, Streaming Media- und RPC-Daten kann ISA Server Datenverkehr je nach Inhalt akzeptieren, ablehnen, weiterleiten oder ändern.
Sichere Serververöffentlichung	Durch die sichere Serververöffentlichung werden Webserver, E-Mail-Server und E-Commerce-Anwendungen vor externen Angriffen geschützt. ISA Server 2004 sorgt durch den Identitätswechsel des

Tabelle 1. Microsoft ISA Server — Die Features auf einen Blick

Feature	Beschreibung
	<p>veröffentlichenden Servers für zusätzliche Sicherheit. Anhand von Webveröffentlichungsregeln können Sie angeben, auf welche Computer zugegriffen werden darf. So schützen Sie Ihre internen Webserver.</p> <p>Mit Hilfe von Serververöffentlichungsregeln können Sie interne Server vor unerwünschtem Zugriff durch externe Benutzer schützen. Alle veröffentlichten Server werden durch die intelligente Anwendungsfiltrierung vor externen Angriffen geschützt.</p>
Erkennung von Eindringversuchen	Mit Hilfe der integrierten Funktionen zur Erkennung von Eindringversuchen, die auf der Technologie von Internet Security Systems basieren, kann ISA Server 2004 bei Erkennung eines Eindringversuchs (z. B. Port Scanning, WinNuke oder Ping of Death) eine Warnung generieren und eine Aktion ausführen.
Integrierte VPN-Funktionen	Die Dienste von ISA Server sind optimal abgestimmt auf die VPN-Dienste von Windows 2000 und Windows Server 2003. So können Sie bei Verbindungen zwischen Zweigstellen und Remotebenutzern mit Ihrem Unternehmensnetzwerk einen standardbasierten, sicheren Remotezugriff gewährleisten. Sie können die ISA Server-Firewallrichtlinie für VPN-Verbindungen verwenden, um genau festzulegen, auf welche Ressourcen und Protokolle VPN-Benutzer zugreifen dürfen.
Firewalltransparenz	Mit SecureNAT ist ein transparenter Firewallzugriff und -schutz für alle IP-Clients gegeben – ohne zusätzliche Clientsoftware oder Konfiguration. Eine interne IP-Adresse wird dabei einfach durch eine global gültige IP-Adresse ersetzt. Hochentwickelte Filter auf Anwendungsebene ermöglichen die Verwaltung von Verbindungen mit umfassender Protokollunterstützung für SecureNAT-Clients.
Sichere Benutzerauthentifizierung	ISA Server 2004 bietet eine sichere Benutzerauthentifizierung mit integrierter Windows-Authentifizierung (Windows NT/LAN Manager und Kerberos) für die Firewall- und Webproxycients. Im Falle von Webproxycients werden Clientzertifikate ebenso unterstützt wie die Digest-, Standard-, formularbasierte und anonyme Webauthentifizierung. ISA Server kann Benutzer anhand der lokalen Firewall- oder Active Directory-Benutzerdatenbank authentifizieren. Auch die Verwendung von Remote Authentication Dial-In User Service (RADIUS) ist möglich.
SSL-zu-SSL-Überbrückung	Für Webserver, bei denen der Clientzugriff über eine Authentifizierung und Verschlüsselung erfolgen muss, bietet ISA Server 2004 uneingeschränkte Sicherheit sowie eine Filterung auf Anwendungsebene mit Hilfe von SSL-zu-SSL-Überbrückung. Anders als die meisten anderen Firewalls kann ISA Server 2004 verschlüsselte Daten überprüfen, bevor sie den Webserver erreichen. Die Firewall entschlüsselt den SSL-Datenstrom, führt eine statusabhängige Überprüfung durch, verschlüsselt die Daten wieder und leitet sie an den veröffentlichten Webserver weiter.
Webcachingserver	
Hochleistungsfähiger Webcache	ISA Server 2004 bietet eine schnelle RAM-Zwischenspeicherung und einen optimierten Datenträgercache für eine schnellere Webleistung – sowohl für den Zugriff auf Internetwebserver durch interne Clients als auch für den Zugriff auf einen Firmenwebserver durch externe Internetbenutzer.
Vorausschauende Zwischenspeicherung	Durch die proaktive Zwischenspeicherung häufig benötigter Objekte stehen den Benutzern aktuelle Webinhalte unmittelbar zur Verfügung. ISA Server 2004 ermittelt automatisch, welche Websites am häufigsten genutzt werden und wie häufig die Inhalte aktualisiert werden sollten. Dabei wird festgestellt, wie lange sich ein Objekt im Zwischenspeicher befunden hat und wann es zuletzt abgerufen wurde. Webinhalte

Tabelle 1. Microsoft ISA Server — Die Features auf einen Blick

Feature	Beschreibung
	können im Voraus in den Zwischenspeicher geladen werden, wenn die Netzwerknutzung gering ist. Dabei muss der Netzwerkmanager nicht anwesend sein. Der Webcache kann auch auf CD oder DVD gespeicherte Offlineinhalte laden.
Zwischenspeicherung nach Zeitplan	Sie können ganze Websites nach einem festen Zeitplan in den Zwischenspeicher laden. Bei solchen geplanten Downloads ist sichergestellt, dass für alle Benutzer die Inhalte im Zwischenspeicher aktuell sind und zudem Inhalte auf Offlinewebsservern zur Verfügung stehen.
Einfache Firewallverwaltung	
Richtlinienbasierte Zugriffssteuerung	Sie können eingehenden und ausgehenden Datenverkehr nach Benutzer, Gruppe, Anwendung, Quelle, Ziel, Inhalt und Zeitplan steuern. Die Assistenten für Firewallrichtlinien geben an, auf welche Websites und Inhalte zugegriffen werden kann, ob sowohl bei ein- als auch bei ausgehender Kommunikation auf ein bestimmtes Protokoll zugegriffen werden kann und ob die Kommunikation zwischen bestimmten IP-Adressen mit den jeweiligen Protokollen und Ports zugelassen oder abgelehnt werden sollte.
Vereinfachte Verwaltung	Mit ISA Server 2004 können Sie die gesamte Firewallkonfiguration in eine XML-Datei kopieren. Indem Sie die Konfigurationsdaten auf Wechselmedien kopieren oder über eine sichere E-Mail an andere Firewalladministratoren senden, können Sie die Firewallkonfiguration für das ganze Unternehmen mühelos standardisieren. Sie können auch einzelne Elemente der Firewallkonfiguration in eine XML-Datei kopieren und anschließend importieren.
Optimale Abstimmung auf Active Directory	Die ISA Server 2004-Firewall kann die in Active Directory gespeicherte Benutzerdatenbank nutzen, um eingehenden und ausgehenden Datenverkehr durch die Firewall zu authentifizieren.
Grafische Taskpads und Konfigurations-Assistenten	Grafische Taskpads und Konfigurations-Assistenten vereinfachen die Konfiguration und die Ausführung allgemeiner Firewallaufgaben. Die Assistenten können z. B. Exchange Server-basierte Server im Netzwerk hinter dem ISA Server 2004-Computer veröffentlichen, die Firewall als VPN-Server oder Gateway konfigurieren oder eine neue Firewallregel festlegen.
Remoteverwaltung	Mit Hilfe der Microsoft Management Console (MMC), mit Windows 2000 Terminaldiensten, Windows Server 2003 Remotedesktop und Befehlszeilenskripts können Sie ISA Server 2004 problemlos über eine Remoteverbindung verwalten. Verfügen Sie über ISA Server 2004-Firewalls unter Windows Server 2003, können Sie für die Remoteverwaltung auch sicheres SSL/RDP Tunneling verwenden.
Protokollierung, Berichterstellung und Warnungen	ISA Server 2004 stellt detaillierte Sicherheits- und Zugriffsprotokolle in standardmäßigen Datenformaten bereit, so z.B. als durch Trennzeichen getrennte Textdatei, SQL-Datenbank, oder MSDE-Datenbank (Microsoft Data Engine). Sie können nach einem bestimmten Zeitplan integrierte Berichte zur Webnutzung, Anwendungsnutzung, zu Netzwerkverkehrsmustern und zur Sicherheit ausführen. Darüber hinaus besteht die Möglichkeit, diese Berichte in einem lokalen Ordner oder einer Remotedateifreigabe automatisch zu veröffentlichen. Ereignisbasierte Warnungen können E-Mail-Nachrichten an Administratoren generieren, Firewalldienste starten und beenden und auf der Basis von Warnungskriterien automatisch Aktionen durchführen.
Verwaltung auf Benutzerebene	Sie können den Zugriff für ISA Server 2004-Webproxy- und Firewallclients nicht nur nach IP-Adressen, sondern auch nach Benutzernamen einschränken. So haben sie eine noch bessere Kontrolle über die eingehende und ausgehende Kommunikation für alle Protokolle.

Tabelle 1. Microsoft ISA Server — Die Features auf einen Blick	
Feature	Beschreibung
Erweiterbare Plattform	
Umfassende Anwendungsunterstützung	ISA Server 2004 unterstützt eine Vielzahl von Internetprotokollen, darunter HTTP/SSL, FTP, RDP, Telnet, RealAudio, RealVideo, IRC, H.323, Windows Media Streaming, E-Mail und News.
Umfassende Produktkompatibilität	Unabhängige Hersteller bieten Produkte an, die auf ISA Server aufbauen bzw. optimal darauf abgestimmt sind, so z. B. Virenerkennungssoftware, Verwaltungstools sowie Inhaltsfilterungs- und Berichterstellungssoftware. Sie können z. B. Filter von Drittanbietern einsetzen, um den Download von neuen Viren, Java-Skripts oder ActiveX®-Steuerelementen auf Ihre gesicherten Netzwerke zu verhindern.
Umfangreiches SDK	ISA Server 2004 stellt ein umfangreiches SDK für die Entwicklung von Tools zur Verfügung, die auf den ISA Server-Firewall-, Caching- und Verwaltungsfeatures aufbauen. Das SDK enthält eine vollständige API-Dokumentation und ausführliche Erläuterungen zur Erstellung zusätzlicher Webfilter, Anwendungsfiler, MMC-Snap-Ins, Berichterstellungstools, skriptbasierter Befehle, Warnungsverwaltungstools usw.

Neue Features in ISA Server 2004

ISA Server 2004 bietet viele neue Features und Verbesserungen, besonders für die Installation auf Systemen unter Windows Server 2003:

- Eine neue, vereinfachte Benutzeroberfläche
- Flexible Unterstützung für unterschiedliche Netzwerk-Designs
- Verbesserte VPN-Unterstützung
- VPN-Quarantänefunktionen
- Möglichkeit zur Erstellung benutzerdefinierter Firewallbenutzergruppen
- Erweiterte Protokollunterstützung
- Individuelle Protokolldefinitionen
- OWA-Veröffentlichungs-Assistent
- Verbesserte Unterstützung für FTP-Upload-/Downloadrichtlinien
- Verbesserte Webveröffentlichung
- Portumleitung für Serververöffentlichungsregeln
- Verbesserte Cacheregeln für eine zentrale Objektspeicherung
- Pfadzuweisung für Webveröffentlichungsregeln
- RADIUS-Unterstützung für Webproxycient-Authentifizierung
- Delegierung der Standardauthentifizierung
- SecureID-Authentifizierung
- Durch die Firewall generierte Formulare (formularbasierte Authentifizierung)
- Verbesserte SMTP-Nachrichtenüberwachung
- Verbesserte HTTP-Filterung

- Linkübersetzung
- Verbesserte Überwachung und Berichterstellung

© 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. Die in den Beispielen verwendeten Firmen, Organisationen, Produkte, Domännennamen, E-Mail-Adressen, Logos, Orte und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Domännennamen, E-Mail-Adressen, Logos, Personen, Orten oder Ereignissen ist rein zufällig.

Microsoft, Active Directory, ActiveX, Outlook, SharePoint, Windows Media und Windows Server System sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Die Namen der in diesem Dokument aufgeführten tatsächlichen Unternehmen und Produkte können geschützte Marken ihrer jeweiligen Inhaber sein.