

Intelligent Application Gateway 2007

Die Komplettlösung für den sicheren Remote-Zugriff

Die Edge Security- und Access-Produkte der Familie Forefront™, der Internet Security and Acceleration (ISA) Server 2006 und das Intelligent Application Gateway (IAG) 2007 leisten einen entscheidenden Beitrag zum Schutz Ihrer IT-Umgebung gegen Gefahren aus dem Internet. Gleichzeitig unterstützen sie Ihre Anwender mit schnellem, policy-basiertem Zugriff auf Unternehmens-Anwendungen und -Daten.

- **Sicherer Remote-Access:**
Zugriff für Mitarbeiter, Partner und Kunden – praktisch unabhängig vom Gerät und Standort
- **Sicherheit für Zweigniederlassungen:**
Verbesserte Connectivity und Sicherheit für Remote-Standorte
- **Internet-Zugriffsschutz:**
Wirkungsvollere Abschirmung der IT-Infrastruktur gegen Gefahren aus dem Internet/Internet-based threats

Zugriffskontrolle

Sicherer, browserbasierter Zugriff auf Unternehmens-Anwendungen und -Daten von mehr Standorten und mit mehr Endgeräten, ohne dass die Installation und Bereitstellung eines Client erforderlich ist.

Schutz der IT-Ressourcen

Der integrierte Anwendungsschutz sichert die Integrität der Netzwerk- und Applikationsinfrastruktur durch Blockierung von schädlichem Datenverkehr und Abwehr von Angriffen.

Sicherung von Informationen

Die durchgängige Policy-Durchsetzung hilft bei der Einhaltung von rechtlichen und unternehmensinternen Vorgaben, die die Kriterien in Bezug auf die Informationsnutzung festschreiben, um die Risiken und Haftungsansprüche beim Zugriff auf sensible Unternehmensdaten zu beschränken.

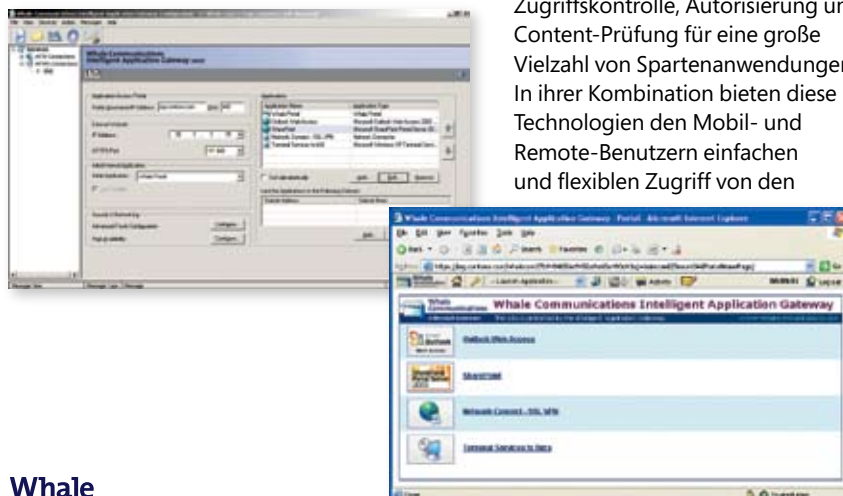
Umfassender sicherer Zugriff

Das Intelligent Application Gateway (IAG) mit Application Optimizer-Modulen stellt ein SSL VPN, eine Web-Applikations-Firewall sowie Funktionalität für das Management der Endpoint-Security bereit und ermöglicht so Zugriffskontrolle, Autorisierung und Content-Prüfung für eine große Vielzahl von Spartenanwendungen. In ihrer Kombination bieten diese Technologien den Mobil- und Remote-Benutzern einfachen und flexiblen Zugriff von den

unterschiedlichsten Orten und Geräten wie Kiosken, PCs und Mobil-Devices. Darüber hinaus ermöglicht das IAG den Administratoren, die Einhaltung von Richtlinien zur Nutzung von Anwendungen und Informationen mithilfe einer speziellen Remote-Zugriffs-Policy durchzusetzen, die sich nach dem Endgerät, dem Benutzer, der Anwendung und nach anderen Unternehmenskriterien richtet.

Integrierte Appliance

Das Intelligent Application Gateway ist eine umfassende, hochleistungsfähige Anwendungszugriffs- und Sicherheits-Appliance, mit der sich die widersprüchlichen Anforderungen in Bezug auf Sicherheit, Anwendungsfunktionalität und möglichst breiten Zugriff ausgleichen lassen. Das IAG bietet nicht nur den Nutzen einer Firewall auf der Netzwerkschicht (Microsoft® Internet Security and Acceleration Server 2006) und eines kompletten SSL VPN, sondern stellt ein policy-gesteuertes Framework bereit, der Endpoint-Sicherheit, Anwendungszugriff und Zugriffskontrolle in einer hoch skalierbaren Plattform vereint, um den Ansprüchen von großen und komplexen Umgebungen gerecht zu werden. Das IAG lässt sich für eine praktisch unbegrenzte Zahl von Benutzern skalieren und bietet Unterstützung für bis zu 64 Hochverfügbarkeits-Knoten in einem Array. Darüber hinaus können die Administratoren komplexe Authentifizierungs-Schemas festlegen, Konfigurationen implementieren, bei denen Session-Überreste rückstandslos gelöscht werden, und ihre eigenen Kriterien für die Endpoint-Compliance definieren. Die Plattform unterstützt mehrere Portale auf einem einzigen Gateway und bietet den Administratoren so die Möglichkeit, die Benutzerführung individuell zu gestalten und spezielle Policy-Konfigurationen für jedes Portal einzurichten.



Intelligent Application Gateway 2007

Zugriffskontrolle

- Flexibles Application-Intelligent-SSL VPN für Zugriff von praktisch jedem Endgerät und Ort aus.
- Differenzierter, policy-gesteuerter Zugriff auf ein breites Spektrum von Netzwerk-, Server- und Daten-Ressourcen.
- Hoch granulare Zugriffs- und Security-Policy.
- Individuell gestaltbare Web-Portal-Präsentation, die sich an der Benutzeridentität orientiert.

Schutz der IT-Ressourcen

- Integration in die Infrastruktur des Unternehmens trägt zur Gewährleistung der Integrität und Sicherheit von Netzwerk-Ressourcen und Anwendungen bei.
- Flexible Web-Applikations-Firewall sorgt für anwendungsspezifische Filterung zum Schutz der Anwendungen gegen unmanaged PCs und Netzwerke.
- Umfassende Überwachung und Protokollierung fördert die Policy-Compliance, indem die Anwenderaktivitäten und die Datennutzung mitverfolgt werden.

Sicherung von Informationen

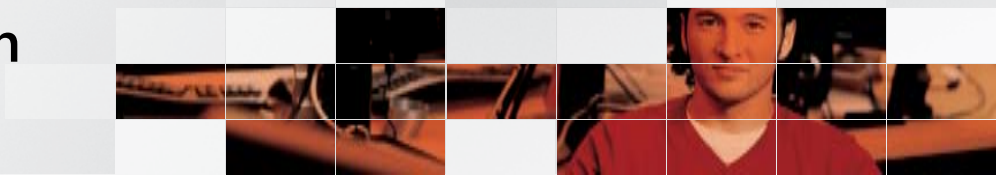
- Konsequentes Management und strikte Überprüfung der Endpoint-Security sichern die Einhaltung von Zugriffs-Policies und Session-Kontrolle.
- Feinmaschigere Kontrolle auf Browser-Ebene über den Zugriff der Benutzer auf Web- und Non-Web-Ressourcen.
- Einhaltung von unternehmensweiten Richtlinien zur Informationsnutzung durch Cache-Bereinigung auf der Client-Seite.

Application Optimizer-Module

Das IAG enthält mehrere sogenannte Intelligent Application Optimizer. Dabei handelt es sich um integrierte Software-Module mit vorkonfigurierten Einstellungen für den sicheren Remote-Zugriff auf häufig genutzte Unternehmensanwendungen. Optimizer bieten Endpoint-Sicherheit, Anwendungs-Publishing und gezielte Filterung von Serveranfragen nach Standardwerten für einzelne Applikationen. Dank dieser Flexibilität können Sie die optimale Balance zwischen dem Erreichen von Unternehmenszielen und der Durchsetzung von Netzwerk- und Daten-Sicherheit erreichen. Bereits integriert sind spezielle granulare Zugriffs-Policy- und Sicherheits-Funktionalitäten für Microsoft Exchange Server und SharePoint® Portal Server sowie für viele Anwendungen von Drittanbietern wie SAP, IBM Domino und Lotus Notes.

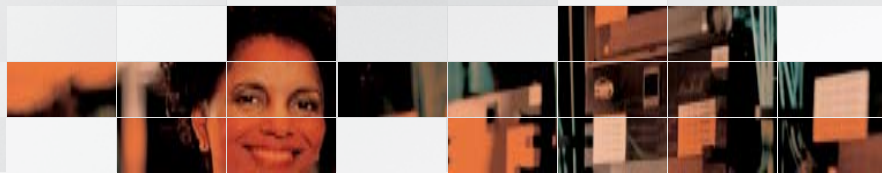
Funktionen	Connectivity		Zugriffs-Policy	Anwendungssicherheit		Endpoint-Sicherheit
	Single Sign-On	Nutzung als Portalseite	Zugriffsbeschränkung auf Anwendungsbereiche	Funktionen blockieren	Anwendungs-Firewall	Attachment Wiper
Application Optimizer	Ja	–	Ja	Upload / Download	Teilweise positivlogisch	Ja
Exchange Outlook® Web Access	Ja	–	Ja	Upload / Download / Bearbeiten	Uneingeschränkt positivlogisch	Ja
SharePoint Portal Server	Ja	–	Ja	Upload / Download	Uneingeschränkt positivlogisch	Ja
Domino Web Access	Yes	Ja	Ja	Upload / Download / Bearbeiten	Teilweise positivlogisch	Ja
IBM WebSphere	Yes	Ja	Ja	Upload / Download / Bearbeiten	Nur negativlogisch	Ja
SAP Portal	Yes	–	Ja	Upload / Download / Exportieren / Bearbeiten	Teilweise positivlogisch	Ja

Intelligent Application Gateway 2007



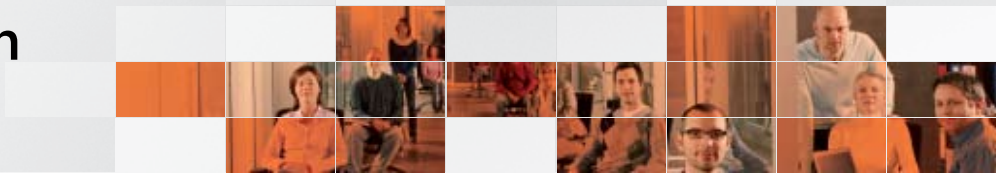
Anwendung	Features
<p>Microsoft SharePoint Portal Server Application Optimizer</p> <p>Das vorkonfigurierte Softwaremodul, das gezielt für SharePoint entwickelt wurde, bietet Out-of-the-Box-Funktionalität, mit der auch der Extranet-Zugriff auf SharePoint über jedes Internet-fähige Gerät möglich ist. Dieser Optimizer stellt Folgendes bereit:</p> <ul style="list-style-type: none"> • Gewährleistung eines kontrollierten Zugriffs für unmanaged Endpoints auf SharePoint, wodurch der Zugriff auch auf Partner und Kunden ausgedehnt wird • Uneingeschränkte Kompatibilität mit Microsoft Office, ohne dass Netzwerk-Tunneling-Komponenten heruntergeladen werden müssen • Integration von Third-Party-, Legacy- oder Client/Server-Anwendungen in den SharePoint Portal Server 	<ul style="list-style-type: none"> • Web-basierter Single Sign-On <ul style="list-style-type: none"> • Web-basierter Single Sign-On beinhaltet Out-of-the-Box-Integration in jedes Repository (auch in mehrere Repositories gleichzeitig), das von SharePoint unterstützt wird (inklusive Native-Support für Microsoft Active Directory®). • Macht mehrere Login-Schritte und Aufforderungen zur Eingabe von Berechtigungsdaten für den Dokumentenzugriff überflüssig. • Integration in den SharePoint Portal Server <ul style="list-style-type: none"> • Damit können die Unternehmen den SharePoint Portal Server als Haupteingang zum Netzwerk nutzen. Nach dem Login wird der Benutzer direkt zum SharePoint Portal Server geleitet. • IAG-Komponenten werden in eine Home-Page des SharePoint Portal Server eingebunden, wobei der Endbenutzerkomfort mit Zugriff auf das IAG-Portal, mit File-Access und mit der IAG Toolbar optimiert wird. • Positivlogische Policy-Durchsetzung <ul style="list-style-type: none"> • Die Anwendungs-Firewall lässt nur bekannte, unbedenkliche Requests an SharePoint Portal Server-Systeme durch und blockiert gleichzeitig Attacken auf der Anwendungsebene wie beispielsweise Cross-Site-Scripting und Buffer-Overflow. • Anwendungsinterne Policy-Durchsetzung <ul style="list-style-type: none"> • Der Policy-Framework ermöglicht die Einschränkung/Zulassung des Zugriffs für die Dokumentenbearbeitung und den Upload bzw. Download von Dateien anhand der Ergebnisse einer Endpoint-Überprüfung.
<p>Microsoft Exchange Server Application Optimizer</p> <p>Der Exchange Server Application Optimizer ermöglicht eine einheitliche Benutzerführung durch die Unterstützung von Windows-basierten Login-Scripts und Single Sign-On, wobei keine mehrfachen Authentifizierungsaufforderungen erforderlich sind. In Kombination mit dem Client/Server Connector-Modul ist der sichere Remote-Zugriff auf den Native Microsoft Outlook® Client mit kompletter Funktionalität möglich, so als würde auf ihn von innerhalb des LAN zugegriffen.</p>	<ul style="list-style-type: none"> • Web Single Sign-On <ul style="list-style-type: none"> • Remote-Zugriffs-Credentials werden an Native-Directories und E-Mail-Repositories weitergegeben, um sicherzustellen, dass Benutzer-Profile und -Berechtigungen durchgesetzt werden. • Single Sign-On und Microsoft Windows®-basierte Logon-Scripts nutzen vorhandene Policy-Logik für eine schnelle Konfiguration. • Endpoint-Sicherheit <ul style="list-style-type: none"> • Attachment Wiper löscht heruntergeladene Seiten und Attachments. • Die Policies in Bezug auf die Anzeige von Attachments basieren auf den Eigenschaften des Endpoint und der Präsenz des Attachment Wiper. • Applikations-Firewall <ul style="list-style-type: none"> • Vorkonfigurierte positivlogische Regeln, die speziell für Exchange Server und IIS geschrieben sind, tragen dazu bei, dass nur legitime Server-Abfragen an nachgeordnete Server weitergegeben werden. • Unterstützt mehrere Versionen von Outlook Web Access und Outlook im Rahmen einer intuitiven, assistentengeführten GUI. • Sicherer Logoff <ul style="list-style-type: none"> • Automatisiert Logoff- und Session-Inaktivitäts-Prompts durch Filtern von Polling-Aktivitäten.
<p>Microsoft Dynamics Optimizer</p> <p>Der Application Optimizer für Microsoft CRM 3.0 ermöglicht sicheres Publishing im CRM Web Portal mit speziellen Policies für die Behandlung CRM-spezifischer Benutzeraktionen, Sicherheitskomponenten und Informationsschutzmechanismen.</p>	<ul style="list-style-type: none"> • Upload/Download-URL-Kontrollen • Eingeschränkte Zonen – Blockade des Zugriffs auf den Settings-Bereich. • Policy-basierte Zugriffskontrolle mit Microsoft CRM 3.0 Enhanced Security <ul style="list-style-type: none"> • Drucken deaktivieren. • Export zu Excel® deaktivieren. • Upload von Attachments zulassen/verweigern.

Intelligent Application Gateway 2007



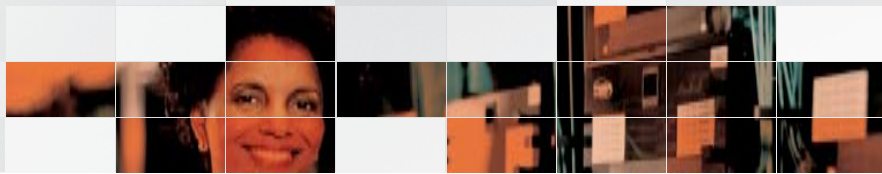
Anwendung	Features
<p>IBM Lotus Domino Web Access Optimizer</p> <p>Mit dem Application Optimizer for IBM Lotus Domino Web Access (DWA) können die Unternehmen die Vorteile von Domino auch außerhalb des LAN uneingeschränkt nutzen. Gleichzeitig dient dieser Optimizer der Wahrung der Anwendungsfunktionalität und zum Schutz der Netzwerkressourcen. Das Gateway leistet auch einen Beitrag zum Schutz der internen Infrastruktur, indem das IP-Adressierungsschema getarnt und interner Domino-Content „on-the-fly“ übersetzt wird.</p>	<ul style="list-style-type: none"> • Policy-gesteuerter Zugriff • Upload/Download von Anhängen kann je nach Endpoint-Profil zugelassen oder blockiert werden. • Automatische Server-Wahl („Jump-Anwendung“) <ul style="list-style-type: none"> • Verbindet die Benutzer mit dem entsprechenden Server für Messaging-Anwendungen in Multi-Server-Umgebungen und sorgt so für transparenten Zugriff. • Endpoint-Sicherheit <ul style="list-style-type: none"> • Cache-Reiniger Attachment Wiper ist so vorkonfiguriert, dass Domino-spezifische Inhalte, die im Cache abgelegt sind, gelöscht werden. • Blockiert Weiterleitung mit Anhängen und E-Mail-History. • Web Single Sign-on <ul style="list-style-type: none"> • Die Benutzer können auf getrennte Domains anhand ihrer Berechtigungen und Zugriffsrechte umgeleitet werden. • Applikations-Firewall <ul style="list-style-type: none"> • Vordefinierter Katalog von Positivregeln lässt nur gültige Kommandos zu. • Anwendungssensitives Logoff- und Session-Inaktivitäts-Prompts durch Ausfiltern normaler Polling-Aktivitäten.
<p>IBM Lotus Domino Optimizer</p> <p>Der IBM Lotus Domino Application Optimizer bietet ein integriertes, vorkonfiguriertes Konzept zur Sicherung und zum Management des externen Web-basierten Zugriffs auf die komplette Serie von IBM Lotus Domino Anwendungen (inklusive Domino Web Access).</p>	<ul style="list-style-type: none"> • Nahtlose Benutzerverbindung <ul style="list-style-type: none"> • Durch die transparente Selektion des Lotus Server und eine eingebaute „Webmail“-Umleitung wird der Benutzer direkt mit dem entsprechenden Server für Messaging-Anwendungen in Multi-Server-Umgebungen verbunden. • Komplette Funktionalität für den Remote-Zugriff <ul style="list-style-type: none"> • Ermöglicht die Verwendung von Lotus Sametime von jedem Access Point aus, auch für nicht-privilegierte Browser, ohne dass ein Tunneling vom Endpoint-Client erforderlich ist. • Dank Unterstützung von Domino Offline Services können E-Mails offline gelesen werden, ohne dass ein kompletter Native-Lotus-Client erforderlich ist. • Ermöglicht die Nutzung des gesamten Lotus Client ausschließlich über HTTPS. • Web-basierter Single Sign-On <ul style="list-style-type: none"> • Remote-Zugriffs-Credentials werden an Native-Directories und Lotus Anwendungen weitergereicht, um die Durchsetzung von Benutzer-Profilen und -Berechtigungen sicherzustellen. • Unterstützung für Authentifizierungs- und Autorisierungs-Add-Ons von Drittanbietern. • Endpoint-Sicherheit <ul style="list-style-type: none"> • Flexibler Policy-Editor bietet die Möglichkeit zur Definition spezieller Überprüfungen auf Lotus Anwendungen wie Sametime oder Domino Offline Services. • Hindert die Benutzer an der Umgehung von Download-Regeln und an der Weiterleitung von Inhalten an externe E-Mail-Accounts. • Applikations-Firewall <ul style="list-style-type: none"> • Vorkonfigurierte positivlogische Regeln, die speziell für Lotus geschrieben sind, tragen dazu bei, dass nur legitime Requests zum Server durchgelassen werden.
<p>SAP Enterprise Portal Optimizer</p> <p>Die SAP-optimierte Lösung bietet granulare, policy-basierte Kontrolle über die Bereiche bzw. Features der SAP-Anwendungen und des SAP Enterprise Portal, auf die der Benutzer zugreifen kann. Das sorgt nicht für höchsten Anwenderkomfort, sondern steigert auch die Sicherheit durch Features wie spezifische Cache-Bereinigung und Session-Timeouts. Dieses Konzept fördert die Produktivität, reduziert die Sicherheitsrisiken und senkt die Kosten.</p>	<ul style="list-style-type: none"> • Policy-gesteuerter Zugriff <ul style="list-style-type: none"> • Upload/Download entsprechend dem Endpoint-Profil. • Das Endpoint-Profil bestimmt, ob Dokumente bearbeitet und gelöscht werden können. • Zugriff auf spezifische iViews – der iView wird nur angezeigt, wenn die Anwendungen dem Benutzer zugewiesen wurden. • Eingeschränkter Zugriff auf persönliche Ordner. • Nahtlose Portalintegration <ul style="list-style-type: none"> • Die Benutzer können nahtlos zu einem Portal mit eigenständigen Policies und sicherem Single Sign-On geleitet werden. • Support für SAP-Applikationen, Anwendungen von Drittanbietern (wie E-Mail), Datenbanken und Legacy-Systeme. • Unterstützung für den Start von einzelnen Anwendungen – die Benutzer müssen sich dabei nicht extra am SSL VPN Portal anmelden. • Umfassende Sicherheit <ul style="list-style-type: none"> • Gesicherter Frontend-Zugriff (Datenverschlüsselung, Reverse-Proxy). • Vorkonfigurierte Anwendungsfilterung (schränkt bestimmte Aktionen auf Backend-Servern, URL-White-Lists ein). • Endpoint-Prüfung. • Spezifische Cache-Bereinigung (lokale Festplatte).

Intelligent Application Gateway 2007



Anwendung	Features		
<p>Mobile Access Optimizer</p> <p>Die Intelligent Application Gateway Lösung für Mobile Access bietet ein sicherheitsoptimiertes Frontend für Exchange Server-Systeme, Datenverschlüsselung und Microsoft ActiveSync® Single Sign-On für E-Mail-Push-Funktionalität. Der Mobile Optimizer stellt eine sicherheitsoptimierte Infrastruktur für ActiveSync, ein mobiles Mikroportal mit Zwei-Faktor-Authentifizierung und Login- und Logout-Prozeduren speziell für mobile Applikationen sowie Anwendungskommando- und URL-Filterung bereit.</p>	<ul style="list-style-type: none"> • Mikroportal für den Mobilzugriff <ul style="list-style-type: none"> • Das Gateway unterstützt ein Standalone-Portal für den Zugriff durch mobile Geräte, wodurch drahtloser Datenverkehr und Internet-basierte Remote-Zugriffs-Aktivitäten getrennt werden können. • Komplette frei gestaltbare Mikroportal-Login-, Portal- und Logout-Seiten. • Single Sign-On für mobile Anwendungen <ul style="list-style-type: none"> • Web-basierter Single-Sign-On automatisiert die ActiveSync Synchronisierung – keine zusätzlichen Login-Schritte wie bei anderen SSL VPN-Implementierungen erforderlich. • Komplette Netzwerktrennung <ul style="list-style-type: none"> • Das Gateway beendet den Datenverkehr in der DMZ und macht so eine Direktverbindung vom Mobilgerät zum Exchange Server überflüssig. • Setzt Benutzer-Authentifizierung und –Autorisierung durch. • Schutz auf der Anwendungsebene <ul style="list-style-type: none"> • Positivlogik-Regeln, die speziell für Outlook Web Access geschrieben sind, stellen sicher, dass nur legitime Server-Requests durchgelassen werden. • Ermöglicht die Definition von eingeschränkten Zonen für Mobilgeräte. 		
<p>Weitere Anwendungen, die ohne Zusatzkonfiguration unterstützt werden</p> <p>Mit speziellem, integriertem Support für mehr als vierzig verschiedene Anwendungen und Services, stellt das IAG eine der umfassendsten Zugriffslösungen bereit, die derzeit verfügbar sind. Vorkonfigurierte Policies, anwendungsspezifische Sicherheitskontrollen und breite Unterstützung für Protokolle erleichtern die Bereitstellung von sicherem Zugriff für die Benutzer auf die unternehmenskritische Infrastruktur ohne zusätzlichen Aufwand.</p>	<table border="0"> <tr> <td> <p>Paketlösungen</p> <ul style="list-style-type: none"> • Windows Terminal Services / Web-Client • IBM Host-On-Demand • IBM WebSphere Portal 5.2 • Lotus Domino Webmail • Lotus Domino Offline Services • Lotus Sametime • PeopleSoft • SAP Enterprise Portal • Citrix Program Neighborhood • Citrix NFuse FR2/FR3 (SecureGateway) • Citrix Presentation Server • Citrix Secure Access Manager • NetManage Rumba Web-to-Host </td> <td> <p>Support für generische Anwendungen</p> <ul style="list-style-type: none"> • Apple Macintosh OS X • Carbon-Anwendungen • Web-basierte und browser-embedded Anwendungen • Client/Server-Applikationen (z.B. RDP, RPC, ...) • HTTP-Proxy-fähige Anwendungen (z.B. Microsoft Live Communications Server) • SOCKS-fähige Client-Anwendungen • Erweiterte Host Address Translation (HAT) • Lokales Laufwerk-Mapping, Web-basierter Dateizugriff • FTP • Telnet </td> </tr> </table>	<p>Paketlösungen</p> <ul style="list-style-type: none"> • Windows Terminal Services / Web-Client • IBM Host-On-Demand • IBM WebSphere Portal 5.2 • Lotus Domino Webmail • Lotus Domino Offline Services • Lotus Sametime • PeopleSoft • SAP Enterprise Portal • Citrix Program Neighborhood • Citrix NFuse FR2/FR3 (SecureGateway) • Citrix Presentation Server • Citrix Secure Access Manager • NetManage Rumba Web-to-Host 	<p>Support für generische Anwendungen</p> <ul style="list-style-type: none"> • Apple Macintosh OS X • Carbon-Anwendungen • Web-basierte und browser-embedded Anwendungen • Client/Server-Applikationen (z.B. RDP, RPC, ...) • HTTP-Proxy-fähige Anwendungen (z.B. Microsoft Live Communications Server) • SOCKS-fähige Client-Anwendungen • Erweiterte Host Address Translation (HAT) • Lokales Laufwerk-Mapping, Web-basierter Dateizugriff • FTP • Telnet
<p>Paketlösungen</p> <ul style="list-style-type: none"> • Windows Terminal Services / Web-Client • IBM Host-On-Demand • IBM WebSphere Portal 5.2 • Lotus Domino Webmail • Lotus Domino Offline Services • Lotus Sametime • PeopleSoft • SAP Enterprise Portal • Citrix Program Neighborhood • Citrix NFuse FR2/FR3 (SecureGateway) • Citrix Presentation Server • Citrix Secure Access Manager • NetManage Rumba Web-to-Host 	<p>Support für generische Anwendungen</p> <ul style="list-style-type: none"> • Apple Macintosh OS X • Carbon-Anwendungen • Web-basierte und browser-embedded Anwendungen • Client/Server-Applikationen (z.B. RDP, RPC, ...) • HTTP-Proxy-fähige Anwendungen (z.B. Microsoft Live Communications Server) • SOCKS-fähige Client-Anwendungen • Erweiterte Host Address Translation (HAT) • Lokales Laufwerk-Mapping, Web-basierter Dateizugriff • FTP • Telnet 		
<p>Application Optimizer Toolkit</p> <p>Der Application Optimizer Toolkit ermöglicht die spezifische Anpassung von Policies für neue Anwendungen und vorhandene Client/Server-Applikationen. Darüber hinaus unterstützt er die tiefgehendere Modifizierung einzelner Optimizer-Modulen, um die Anforderungen einer speziellen Unternehmens-Implementierung zu erfüllen.</p>	<ul style="list-style-type: none"> • Erweiterung vorhandener Optimizer-Module, um Standardkonfigurationen für spezielle Unternehmensanforderungen auszubauen und neue, individuelle Policies und Content-Regeln für intern entwickelte Anwendungen zu erstellen. • Das IAG bietet anspruchsvolle Policy-Editor-Features zur Unterstützung der Administratoren bei der Definition von komplexen Compliance-Checks wie beispielsweise die Überprüfung auf Antiviren-Updates, die in der letzten Woche durchgeführt wurden. Der Advanced Policy Editor ermöglicht den Administratoren die Verwendung Boolescher Operationen und neuer Variablen bei der Definition von Policies. Dadurch entfällt das arbeitsaufwändige Policy-Management, bei SSL VPN-Appliances von Mitbewerber erforderlich ist. 		

Intelligent Application Gateway 2007

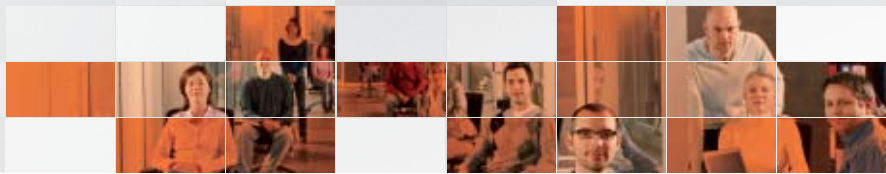


Product Features

Skalierbarkeit	
Benutzer	Unterstützung für eine unbeschränkte Zahl von Benutzern auf einem einzigen Gateway.
Hohe Verfügbarkeit	Lässt sich linear auf bis 64 High-Availability-Knotenkonfigurationen skalieren.
Verwaltungsfunktionalität	
Flexibilität	Wird mit Standard-Softwarekonfigurationen für die gängigsten Unternehmensanwendungen ausgeliefert und ermöglicht auch die individuelle Anpassung, beispielsweise mit Authentifizierungs-, Autorisierungs- und Endpoint-Compliance-Profilen oder kontextsensitiven Web-Portalen. Unterstützung für Positivlogik-Rule-Sets und Anpassung von URL-Filtern sowie die Möglichkeit, Regelkataloge für modifizierte oder proprietäre Anwendungen zu entwickeln.
SSL VPN-Portal	Stellt einen praktischen Single-Access-Point für Anwendungen bereit, unterstützt aber auch mehrere Access-Points mit eigenen Policy-Parametern wie Partner-Extranets und Mitarbeiterportale auf einem einzigen Gateway.
Protokollierung und Reporting	Unterstützt die Überwachung, die Protokollierung und das Reporting für Management und Accounting auf Unternehmensebene (System, Benutzersicherheit und Session-Views): <ul style="list-style-type: none"> • Event Monitor bietet umfassende Ereignisüberwachung, die nach Benutzer, Anwendung oder Zeitraum strukturiert ist. • Integrierter Event Logger, der die Systemnutzung und Anwenderaktivitäten protokolliert und Warnhinweise bezüglich sicherheitsrelevanter Ereignisse an eine Verwaltungskonsole schickt. • Integriertes Event Query Tool mit vorkonfigurierten Templates und voller Reporting-Funktionalität.
Umfassender Policy-Framework	<ul style="list-style-type: none"> • Out-of-the-Box-Einstellungen für den Anwendungszugriff und Endpoint-Policy-Konfigurationen, um minimalen Integrationsaufwand und niedrige laufenden Verwaltungskosten zu gewährleisten. • Unterstützung des Intelligent Application Toolkit für die Definition von Positivlogik-Regelkatalogen und URL-Filtern zur Ergänzung der Optimizer-Einstellungen und Entwicklung von Policies für modifizierte oder proprietäre Anwendungen. • Unterstützung des Intelligent Application Template, das einen Framework zur Entwicklung eines Application Optimizer für generische Web-Anwendungen und auch für komplexe Enterprise-Applikationen mit Komponenten, Web-Parts und Objekten bereitstellt.
Access Policy	
Endpoint-Compliance-Prüfungen	Endpoint-Policy ermöglicht den Administratoren die Definition von Compliance-Prüfungen anhand von vorkonfigurierten Variablen wie beispielsweise die Präsenz von Sicherheits-Software und IAG-spezifischen Applikationen wie Attachment Wiper. Unterstützung für komplexe Endpoint-Policy-Regeln mit individuell gestaltbaren Compliance-Checks, bei denen Boolesche Operationen genutzt werden können.
Anwenderkomfort	<ul style="list-style-type: none"> • Bereitstellung eines Standard-SSL-VPN-Portals und von Login-Seiten, was eine einfache Konfiguration ermöglicht und niedrige Verwaltungskosten gewährleistet. • Unterstützung für die Gestaltung des Portals und der Login-Seiten nach dem Vorbild des vorhandenen Intranet. Erfordert keine Einhaltung der Vorgaben eines Vendor-Portal-Template.
Integriertes Zertifikatsstellen-Management	Bietet eine eingebaute Zertifikatsstelle, falls der Administrator keine externe Zertifikatsstelle nutzen will. Ermöglicht den Administratoren, auf Anforderung ein Trusted-Endpoint-Zertifikat für einen bestimmten Rechner auszustellen.



Intelligent Application Gateway 2007

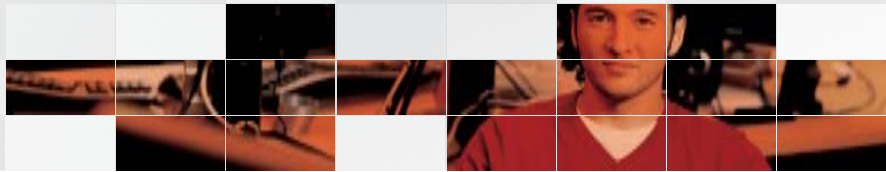


Vorteile einer integrierten Lösung

Bei Ihrer Wahl der Zugriffsmethode sollten Sie sich sowohl von Unternehmens- als auch von Sicherheitsanforderungen leiten lassen. Ziel von Microsoft ist die Bereitstellung einer flexiblen Lösung, die sich problemlos an die unterschiedlichsten Nutzungs- und Implementierungsszenarien anpassen lässt.

Implementierung	ISA Server (2006) Standalone	Intelligent Application Gateway 2007
Sicherheit für Zweigstellen	<ul style="list-style-type: none"> Gateway für die Verbindung von Standorten und Gewährleistung der Sicherheit 	<ul style="list-style-type: none"> Bereitgestellt vom ISA Server
	<ul style="list-style-type: none"> Internet-Zugriffskontrolle durch das Rechenzentrum und Web-Caching mit einer Firewall, die komplett in der Netzwerkschicht implementiert ist 	<ul style="list-style-type: none"> Bereitgestellt vom ISA Server
Control Access		
Schutz des Internet-Zugriffs	<ul style="list-style-type: none"> Publizierung und Sicherung spezifischer Web-Anwendungen und Vorauthentifizierung des Zugriffs darauf (Exchange Server, SharePoint Server) 	<ul style="list-style-type: none"> Differenzierter und policy-gesteuerter Zugriff auf praktisch alle Anwendungen, Netzwerke, Serversysteme oder Datenressourcen Zugang zu flexiblem „Application-Intelligent“-SSL VPN für jedes Gerät und für jeden Standort Äußerst granulare Zugriffs- und Sicherheitspolicy, die auch mit anwendungsinternen Kontrollmechanismen arbeitet Individuell gestaltbare Web-Portal-Präsentation, die sich an der Benutzeridentität orientiert
	Schutz von IT-Ressourcen	
Sicherer Remotezugriff	<ul style="list-style-type: none"> Schutz des Edge-Bereichs des Netzwerks durch Stateful Packet Inspection Anwendungsschutz mit anspruchsvoller Protokollfilterung und Prüfung 	<ul style="list-style-type: none"> Tiefgehende Content-Prüfung und Filterung mit Eingabe-Validierung und granularen Upload/Download-Kontrollen Anpassbare Web-Applikations-Firewall setzt anwendungsspezifische Filterung durch und schützt Applikationen gegen unmanaged PCs und Netzwerke Integration in Unternehmens-Infrastruktur trägt zur Wahrung der Integrität und Sicherheit der Netzwerk-Ressourcen und Anwendungen bei Umfassende Überwachung und Protokollierung leistet Beitrag zur Policy-Einhaltung durch Mitverfolgung der Anwenderaktivitäten und Datennutzung
	Sicherung von Informationen	
	<ul style="list-style-type: none"> Uneingeschränkte IPsec VPN Netzwerk-Connectivity ist in Firewall-Engine für Zugriff durch managed PCs integriert 	<ul style="list-style-type: none"> Uneingeschränkter Netzwerkzugriff auf Browser-Basis Konsequentes Management und strikte Überprüfung der Endpoint-Security sichern die Einhaltung von Zugriffs-Policies und gewährleisten die Session-Kontrolle Feinmaschigere Kontrolle im Browser über den Zugriff der Anwender auf Web- und Non-Web-Ressourcen Erfüllung der Unternehmensrichtlinien zur Informationsnutzung durch Datenbereinigung auf der Client-Seite

Intelligent Application Gateway 2007



Connectivity-Module

Client/Server Connector

Der Client/Server Connector bietet sicheren Out-of-the-Box-Zugriff auf unternehmenskritische Client/Server-Anwendungen wie Microsoft Exchange, Lotus Notes native client, Citrix, Microsoft Terminal Services, FTP und Telnet. Gleichzeitig ermöglicht er die einfache Konfiguration für weitere Client/Server-Applikationen mithilfe eines generischen Anwendungs-Definitions-Tools.

Tunneling-Modi

- **Port Forwarding:** Die Client-Komponente fragt eine spezifische lokale Adresse samt Port für jede Anwendung ab und weist die Applikation an, den TCP-Traffic zu dieser Adresse zu schicken, anstatt zur wirklichen IP-Adresse des Anwendungsservers. Der SSL VPN-Client kapselt dann den abgefangenen Datenverkehr innerhalb von SSL und schickt ihn zum Gateway. Dieser Modus funktioniert am besten bei Anwendungen, die statische TCP-Ports nutzen, bzw. bei Applikationen, die einen HTTP- oder SOCKS-Proxy unterstützen.
- **Socket Forwarding:** Die Clientkomponente klinkt sich in die Server-Provider-Schnittstelle Winsock von Microsoft ein. Sie nutzt Windows LSP/NSP-Schnittstellen (Layered Service Provider/Name Space Provider) für das Socket-Handling auf unterer Ebene. NSP dient der Auflösung von internen Servernamen, um sicherzustellen, dass sie getunnelt werden. Diese Methode bietet uneingeschränkte Unterstützung für alle Winsock-Anwendungen – TCP und dynamische Ports.

Network Connector

Der Network Connector ermöglicht den Administratoren die Installation, den Betrieb und das Management von Remote-Verbindungen, die den Benutzern transparente Connectivity bieten, die als virtuelle und security-fähige Verbindung komplett auf der Netzwerkschicht realisiert ist. Die Anwender können damit die gleiche Funktionalität nutzen wie bei einer Direktverbindung zum Unternehmensnetzwerk.

- Das Network Connector-Modul vergibt eine lokale IP-Adresse an externe Benutzer, so als befänden sie sich im Netzwerk. Damit können sie remote auf Unternehmens-Server und komplexe Systeme wie File-Shares und interne Datenbanken über eine sicherere Verbindung auf der Netzwerkschicht zugreifen (Shared Folders).
- Das Network Connector-Modul tunnelt praktisch jedes IP-basierte Protokoll und bietet damit auch Support für Voice over IP (VoIP).
- Die Fähigkeit des Network Connector, eine Direktverbindung zu Abteilungsservern anhand der Identität des Benutzers aufzubauen, bietet erhebliche Sicherheitsvorteile, da keine vollständig offene Verbindung auf der Netzwerkschicht für alle Benutzer durch das SSL-VP-Gateway direkt zum LAN erforderlich ist.
- Die Administratoren haben die Option, die Verbindung im direkten Anschluss an das Benutzer-Login mithilfe eines vordefinierten Script nach einem Compliance-Check aufzubauen. Es ist auch eine On-Demand-Verbindung durch den Benutzer möglich, indem er nach der Autorisierung das Network Connector-Symbol auf der Portalseite anklickt.

Das Beste beider Welten

Das IAG 2007 ist in den ISA Server 2006 integriert und stellt eine konsolidierte Appliance für den Schutz des Netzwerk-Perimeters, für den Remote-Zugriff und für den Schutz von SSL- und IPsec-Verbindungen auf der Ebene der Anwendungsschicht bereit. Die Unternehmen profitieren damit von einer breiteren Auswahl bei der Erfüllung ihrer Anforderungen an den Remote-Zugriff. Durch die Integration von SSL VPN in die vorhandene Microsoft-Infrastruktur wird sicherer Zugriff auf Microsoft- und Non-Microsoft-Anwendungen und -Services über eine einzige Appliance unterstützt. Die IAG 2007 Appliance überzeugt durch ein neues optimiertes und kostengünstiges Design, das zur Senkung der Betriebskosten beitragen kann und die Installation von

mehreren Geräten verschiedener Anbieter für unterschiedliche Zugriffsmethoden überflüssig macht. Die zentrale IT-Abteilung kann jetzt eine konsolidierte Sicherheits-Appliance-Lösung einführen, die flexibel und leicht zu implementieren ist.

Die Sicherung des Perimeters

In Kombination mit dem Intelligent Application Gateway unterstützt der ISA Server die notwendige Netzwerktrennung und ermöglicht die Kontrolle von ein- und ausgehendem Content. Gleichzeitig bietet er wichtige zusätzliche Funktionalität zur Sicherung des Edge-Bereichs, um einer breiten Palette von Internet-Gefahren vorzubeugen. Die konsolidierte Appliance stellt eine flexible, softwaregesteuerte Lösung bereit, die die Forderungen nach Performance, Management, Skalierbarkeit und umfassender Sicherheit gleichermaßen abdeckt. Die Kombination aus Stateful Packet Filtering, Circuit Filtering, Filterung auf der Anwendungsschicht, Web Proxy und Endpoint-Sicherheit in einer einzigen Appliance eröffnet dem Administrator eine Vielfalt von Optionen zur Konfiguration von policy-gesteuertem Zugriff auf Anwendungen und Netzwerkressourcen.

Anstatt mit einer mechanistische Lösung zu arbeiten, bietet der ISA Server die Möglichkeit, den Verkehr zu filtern, wodurch drei Arten der Firewall-Funktionalität zur Verfügung gestellt werden: Packet Filtering (auch Circuit-Layer Filtering genannt), Stateful Filtering und Application-Layer Filtering. Die Fähigkeit, regelbasierte Filterung auf den gesamten Verkehr anzuwenden, der die Netzwerkgrenze überquert, ermöglicht eine kombinierte Lösung zur direkten Abwehr von Gefahren wie Würmern oder Malware, die von authentifizierten Benutzern ausgehen könnten.

Powered by:

Microsoft®
**Internet Security &
Acceleration Server 2006**

Weiter Informationen zum Intelligent Application Gateway 2007 finden Sie unter <http://www.microsoft.com/iag>.

Dieses Datenblatt dient ausschließlich Informationszwecken. MICROSOFT SCHLIESST JEGLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG IN BEZUG AUF DIE AUSSAGEN IN DIESEM DATENBLATT AUS.

© 2007 Microsoft Corporation