

Warum einen IAG Server? Und warum als Appliance?



Microsoft®
**Internet Security &
Acceleration Server**

Microsoft Intelligent Application Gateway 2007 auf einer Celestix WSA Appliance Celestix hat für Microsofts Intelligent Application Gateway eine leistungsfähige Appliance entwickelt – Die Celestix WSA -Appliance.

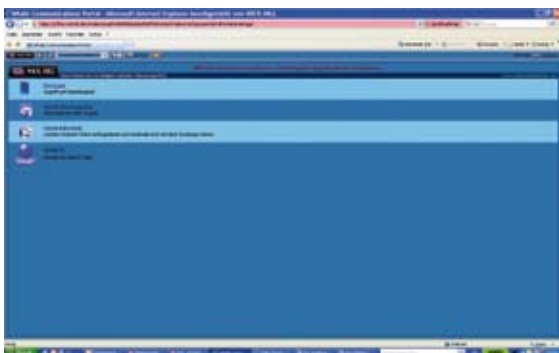
Mit dem IAG kombiniert Microsoft den ISA Server 2006 und das Intelligent Application Gateway der Firma Whale Communications zu einer performanten und gleichzeitig sicheren Fernzugriffslösung über SSL-VPN. Die Edge Security- und Access-Produkte der Microsoft Forefront-Familie, der Internet Security and 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**

Mit dem Intelligent Application Gateway können Sie Ihren Anwendern ein Portal zur Verfügung stellen, auf dem über eine SSL-VPN Verbindung die Anwendungen bereitgestellt werden. Durch die Firewallinstanz des ISA-Servers wird bei der IAG-Appliance volle Sicherheit gewährleistet. Sie können das Portal optisch an Ihre Firma anpassen und alle Icons etc verwenden, die sie möchten.

Mit einem IAG haben Sie außerdem die Möglichkeit, den Zugriff granular zu steuern. Somit können Sie nicht nur den Zugriff per Authentifizierung oder Zertifikat gewährleisten, sondern Sie können auch bestimmen, welche Softwarepakete installiert sein müssen für einen vollen Zugriff, welchen Signaturstand das Antivirenprogramm hat und auf welchem Windows Patchlevel der Client steht.

Ob Internetcafe, Firmenlaptop oder fremdes Firmennetzwerk: Das IAG schafft Transparenz und Sicherheit, weil die Clients beim Zugriff überwacht werden und der Umfang des Zugriffes vorher festgelegt wird. Diese Endpoint-Überprüfung ist an Ihre Bedürfnisse anpassbar und eines



der wichtigsten Features des IAG. Erfüllt ein Client Ihre Anforderungen nicht, werden seine Zugriffsrechte heruntergesetzt um Datenverluste zu minimieren. Erfüllt der Nutzer alle Ihre Anforderungen, kann er über das IAG-Portal von zu Hause aus so arbeiten, als säße er im Büro. Nachdem der Nutzer sich ausgeloggt hat, werden alle Sitzungsrückstände von seinem Client entfernt.

Wenn Sie ein Intelligent Application Gateway nutzen, müssen Sie nicht zwei Instanzen konfigurieren (ISA und IAG), weil dies der IAG-Server übernimmt. Das heißt, dass man auf dem ISA-Server keinerlei Policies konfigurieren muss um die Erreichbarkeit des IAG-Portals zu gewährleisten.

Den Möglichkeiten bei der Einrichtung der Policy sind mit einem Intelligent Application Gateway keine Grenzen gesetzt – Sie können die Freigabe von Anwendungen auf Gruppen und einzelne Nutzer herunter brechen und hier jeweils nach den sich einwählenden Clients unterscheiden.

Alle Celestix Appliances verfügen über eine versteckte Partition, von der aus Sie Ihre Appliance auf „Factory Default“ oder eine von Ihnen abgespeicherte „Last Good Version“ zurücksetzen können. Hiermit werden Ihnen Ausfallzeiten erspart. Die Konfiguration des ISA-Servers kann außerdem auch noch auf ein gesondertes Backup gesichert werden.

Celestix baut für Microsoft hochwertige Appliances, auf denen sowohl ein gehärteter Windows Server 2003, als auch der ISA/ IAG Server bereits installiert ist. Ergänzt wird die Box durch eine von Celestix entwickelte Web-Oberfläche zur Fernwartung des jeweiligen Servers.

Sie können Ihren Kunden eine geschlossene Komplettlösung bereitstellen – Sie müssen nichts mehr installieren und haben keinen Ärger mehr mit überflüssigen Bestandteilen des Betriebssystems. Sie kaufen alle Lizenzen zusammen: Hardware, Betriebssystem & Software und haben nur einen Supportweg. Sie können optional Kaspersky Antivirus und WebSense Websecurity einbinden, die Produkte stehen auf der Appliance zum Download bereit und integrieren sich nach der Installation in die Weboberfläche.

Das Upgrade auf das Unified Access Gateway (UAG) – dem Nachfolger vom IAG Server ist in dem Support bereits enthalten – Sie bekommen dann von Celestix das Image des neuen Betriebssystems und die neue Software. Die Konfiguration werden Sie übernehmen können. Das UAG soll Anfang des Jahres 2010 auf den Markt kommen.





Umfassende und sichere Fernzugriffslösung

Bei den WSA™ SSL VPN-Appliances von Celestix™ handelt es sich um hochleistungsfähige Zugriffssicherheitslösungen. Diese bieten auf der einen Seite ein Höchstmaß an Schutzvorkehrungen und garantieren auf der anderen Seite einen einfachen Zugriff von außerhalb auf unternehmenskritische Anwendungen.

Wir leben heute in einer Welt, in der es in virtuellen Umgebungen keine Grenzen mehr gibt. Um eine möglichst hohe Effizienz zu gewährleisten, müssen Unternehmen ihren Mitarbeitern einen zuverlässigen Zugriff auf das Netzwerk garantieren, unabhängig von Standort und Zeit. Informationen und Daten werden zum höchsten Gut für ein Unternehmen und der Remote Access auf das Netzwerk damit zu einem absoluten „Muss“. Außendienstmitarbeiter eines Unternehmens sind auf den uneingeschränkten Zugriff auf Anwendungen wie E-Mail, Auftragserfassung und -status, Instant Messaging und Intranet angewiesen, damit der Geschäftsbetrieb stabil und zuverlässig funktioniert. Unternehmenskritische Daten gilt es massiv zu schützen. Innerhalb der Firmenmauern scheint diese Übung noch relativ überschaubar – schwierig wird es jedoch einen Zugriff von außerhalb abzusichern. Hier spielen viele Komponenten, die nur schwer zu kontrollieren sind, eine gewichtige Rolle. Angriffe über das Internet gehören zum am schnellsten wachsenden Bereich der Cyber-Kriminalität. Deshalb müssen sämtliche Unternehmen, ob groß oder klein, stets wachsam sein. Die WSA SSL VPN-Anwendungen von Celestix unterstützen IT-Verantwortliche in ihrem Bemühen, die Zugänglichkeit der Informationsbestände so zur Verfügung zu stellen, wie es gewünscht wird. Das heißt, auf der einen Seite nur den tatsächlich autorisierten Anwendern einen Zugriff zu erlauben, und gleichzeitig vor äußeren Attacken zu schützen. Die Celestix WSA-Appliance kombiniert die Leistungsfähigkeit der Celestix Scorpio-Anwendungshardware und der Engine-Software „SlingSHOT™“ mit Microsofts Intelligent Application Gateway 2007 und dem Internet Security and Acceleration Server 2006. Zusammen bilden sie die derzeit fortschrittlichste, auf dem Markt erhältliche SSL-Zugriffslösung für Virtual Private Networks (VPN).

ZUGRIFFSKONTROLLE

Sichere und zuverlässige Authentifizierung - schützt die Anwender vor unliebsamen Attacken und beschleunigt den Zugriff für autorisierte Benutzer.

SCHUTZ DER RESSOURCEN

Der integrierte Anwendungsschutz gewährleistet die Unversehrtheit und Sicherheit der Netzwerk- und Anwendungsinfrastruktur.

ABSICHERUNG VON INFORMATIONEN

Die konsequente Durchsetzung von Richtlinien (Policies) hilft bei der Einhaltung gesetzlicher und unternehmens-interner Anforderungen (Compliance). Auf diese Weise werden Risiken und Verantwortlichkeiten beim Zugriff auf sensible Unternehmensdaten minimiert.

DIE WICHTIGSTEN MERKMALE AUF EINEN BLICK

- Einfach zu installierende und sichere Fernzugriffslösung
- Eine einzige Plattform für den Fernzugriff von Mitarbeitern und Geschäftspartnern
- Zugriff auf Unternehmensanwendungen und -ressourcen - unabhängig vom Client
- Branchenführende Endpunktsicherheit, einmalige Anmeldung für Web-Anwendungen (Single Sign-On), granulare Zugriffskontrolle und Schutz vor Bedrohungen (Threat Prevention)
- Die skalierbaren Anwendungen werden den Fern- und Extranet-Zugriffsanforderungen von Unternehmen jeder Größe gerecht
- Web-basierte, grafische Benutzeroberfläche (GUI) für die Fernverwaltung
- Frontpanel mit LC-Display zur einfachen Netzwerkkonfiguration und Statusanzeige
- One button-System zur Wiederherstellung der Werkseinstellungen und letzten fehlerfreien Version
- Echter Gigabit-Netzwerkdurchsatz
- PCI-Express-Architektur
- Update-Services

UMFASSENDE UND SICHERER ZUGRIFF

Die WSA-Appliance beinhaltet folgende Features: SSL-VPN, eine Firewall für Web-Anwendungen sowie einen Endpoint-Security Ansatz, der Zugriffskontrolle, Autorisierung und Inhaltsprüfung für eine Vielzahl von Geschäftsanwendungen ermöglicht. Zusammen sorgen diese Funktionalitäten dafür, dass mobile Mitarbeiter und Außendienstmitarbeiter von einem breiten Spektrum von Geräten und Standorten, wie öffentlich zugänglichen Computern, PCs und mobilen Geräten, auf einfache und flexible Weise von einem sicheren Zugriff profitieren können. WSA ermöglicht es IT-Administratoren außerdem, die Einhaltung von Richtlinien zur Nutzung von Anwendungen und Informationen mithilfe einer benutzerdefinierten Remote-Access-Policy (Fernzugriffsrichtlinie) umzusetzen.

Funktion	Konnektivität		Zugriffsrichtlinie	Anwendungssicherheit		Endpoint Security
	Single Sign-on	Nutzung als Portalseite	Zugriffsbeschränkung auf Anwendungsbereiche	Funktionen sperren	Anwendungs-Firewall	Attachment Wiper
Application Optimizer						
Exchange Outlook Web Access	ja	k.A.	ja	Upload/ Download	Teilweise positiv	ja
SharePoint Portal Server	ja	ja	ja	Upload/ Download/Bearbeiten	Uneingeschränkt positiv logisch	ja
Domino Web Access	ja	k.A.	ja	Upload/ Download	Uneingeschränkt positiv logisch	ja
IBM WebSphere	ja	ja	ja	Upload/ Download/Bearbeiten	Teilweise positiv	ja
SAP Portal	ja	ja	ja	Upload/ Download/Bearbeiten	Nur negativ	ja
EMC Documentum Webtop	ja	ja	ja	Upload/ Download/Bearbeiten	Teilweise positiv	ja
Dynamics	ja	k.A.	ja	Upload/ Download/Bearbeiten/ Exportieren	Teilweise positiv	ja

Konnektivitätsmodule

CLIENT/SERVER CONNECTOR

Der Client/Server Connector bietet sofort einen sicheren Zugriff auf geschäftskritische Client-/Server-Anwendungen wie Microsoft Exchange, Lotus Notes, Citrix, Microsoft Terminal Services, FTP und Telnet. Gleichzeitig gewährleistet er eine einfache Konfiguration für weitere Client-/Server-Anwendungen dank eines generischen Tools zur Anwendungsdefinition.

TUNNELING-MODI

- **Port-Weiterleitung (Port Forwarding):**
Die Client-Komponente reagiert auf eine spezifische lokale Adresse an einem bestimmten lokalen Port und veranlasst die Anwendung, den TCP-Datenverkehr an diese Adresse zu senden und nicht an die echte IP-Adresse des Anwendungsservers. Der SSL VPN-Client kapselt den abgefangenen Datenverkehr ein und schickt diesen dann verschlüsselt zum Gateway. Dieser Modus funktioniert optimal bei Anwendungen, die statische TCP-Ports nutzen, oder bei Anwendungen, die einen HTTP- oder SOCKS-Proxy unterstützen.
- **Socket-Weiterleitung (Socket Forwarding):**
Die Client-Komponente koppelt sich mit der SPI-Schnittstelle (Service Provider Interface) von Microsoft Winsock. Sie nutzt die LSP-/NSP-Schnittstellen (Layered Service Provider/Name Space Provider) von Windows und bietet Socket-Handling auf niedriger Ebene. Zudem zeichnet sie sich durch die volle Unterstützung sämtlicher Winsock-Anwendungen aus – wie TCP und dynamische Ports.

APPLICATION OPTIMIZER

WSA beinhaltet mehrere Intelligent Application Optimizer: Integrierte Softwaremodule mit vorkonfigurierten Einstellungen für den sicheren Fernzugriff auf häufig genutzte Unternehmensanwendungen. Diese Optimizer bieten Endpoint-Security, Application Publishing und Filterung von Serveranfragen nach Standardwerten für individuelle Anwendungen. So soll ein flexibles Gleichgewicht zwischen einem effizienten Geschäftsablauf bei maximaler Netzwerk- und Datensicherheit erreicht werden. Standardmäßig integriert sind benutzerdefinierte, granulare Zugriffsrichtlinien- und Sicherheitsfunktionen für Microsoft Exchange Server und SharePoint® Portal Server sowie für zahlreiche Geschäftsanwendungen wie SAP, IBM Domino und Lotus Notes.

NETWORK CONNECTOR

Der Network Connector erlaubt es Administratoren, Fernverbindungen zu installieren, zu betreiben und zu verwalten, die Nutzern über eine virtuelle, sichere und transparente Verbindung die volle Konnektivität auf Netzwerkebene bieten. Darüber hinaus profitieren die Nutzer von derselben Funktionalität, als wären sie direkt mit dem Unternehmensnetzwerk verbunden.

- Das Network-Connector-Modul weist externen Nutzern eine lokale IP-Adresse zu. So können sie aus der Ferne über eine sichere Verbind-

gung auf Netzwerkebene (gemeinsame Ordner) auf Unternehmensserver und komplexe Systeme wie File Shares und interne Datenbanken zugreifen.

- Das Network-Connector-Modul tunnelt nahezu jedes IP-basierte Protokoll und unterstützt daher auch Voice over IP (VoIP).
- Die Fähigkeit des Network Connectors, auf Grundlage der Benutzeridentität eine Direktverbindung zu den unterschiedlichen Servern in den Abteilungen herzustellen, hat beträchtliche Vorteile für die Sicherheit, weil keine vollkommen offene Verbindung auf Netzwerkebene vom SSL VPN-Gateway direkt zum LAN für alle Nutzer notwendig ist.
- Er bietet Administratoren die Möglichkeit, die Verbindung unmittelbar nach der Benutzeranmeldung (User Login) mithilfe eines vordefinierten Scripts, nach einer Compliance-Prüfung oder auf Abruf seitens des Benutzers aufzubauen, indem dieser nach der Autorisierung das Network-Connector-Symbol auf der Portalseite anklickt.

VON DEN VORTEILEN BEIDER SEITEN PROFITIEREN

Die WSA mit dem integrierten ISA Server 2006 stellt eine gemeinsame Anwendung für den Schutz des Netzwerkperimeters, des Fernzugriffs und der SSL- und IPsec-Verbindungen auf Anwendungsebene zur Verfügung. Die Integration von SSL VPN in die bestehende Microsoft-Infrastruktur unterstützt den sicheren Zugriff auf die Anwendungen und Services von Microsoft und anderen Anbietern über eine einzige Anwendung. Die WSA-Appliance zeichnet sich durch ein neues, verbessertes und kostengünstiges Design aus, das die Betriebskosten reduzieren hilft und die Nutzung mehrerer Geräte von unterschiedlichen Anbietern für verschiedene Zugriffsmethoden überflüssig macht. Die IT-Abteilung Ihres Unternehmens kann nun eine konsolidierte Sicherheitslösung einführen, die flexibel und einfach einzusetzen ist.

PERIMETERSCHUTZ

Der ISA Server sorgt in Verbindung mit dem Intelligent Application Gateway (IAG) für die erforderliche Netzwerktrennung und die Überwachung von ein- und ausgehenden Inhalten. Dabei bietet er zusätzliche Funktionalität für den Schutz des Netzwerkes, um eine Vielzahl von Internet-Bedrohungen abzuwehren. Die konsolidierte Anwendung stellt eine flexible, softwaregesteuerte Lösung dar, die neben umfassender Sicherheit auch der Forderung nach Leistungsfähigkeit, Verwaltbarkeit und Skalierbarkeit gerecht wird. Die Kombination von Stateful Packet Filtering, Circuit Filtering, Application-Layer Filtering, Web-Proxy und Endpunktsicherheit in einer einzigen Anwendung gibt dem Administrator vielfältige Möglichkeiten zur Konfiguration eines richtliniengesteuerten Zugriffs auf Anwendungen und Netzwerkressourcen.

ISA Server bietet die Möglichkeit zur Filterung des Datenverkehrs, anstatt mit einer mechanistischen Lösung aufzuwarten. Dabei werden drei Arten von Firewall-Funktionalitäten bereitgestellt: Packet Filtering auch Circuit-Layer Filtering genannt, Stateful Filtering und Application-Layer Filtering. Dank der Fähigkeit, eine regelbasierte Filterung auf den gesamten Datenverkehr anzuwenden, der die Netzwerkgrenze passiert,

kann die konsolidierte Lösung Bedrohungen wie beispielsweise Würmer oder Malware, die von authentifizierten Benutzern ausgehen können, direkt abwehren.

Produktmerkmale

SKALIERBARKEIT

Benutzer: Unterstützt eine unbegrenzte Benutzeranzahl auf einem einzigen Gateway.

Hochverfügbarkeit: Linear skalierbar auf bis zu 64 hochverfügbare Knotenkonfigurationen.

ZUGRIFFSRICHTLINIE

Endpunkt-Compliance-Prüfungen





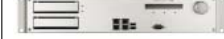
Die Endpunktrichtlinie erlaubt es Administratoren, Compliance-Prüfungen mithilfe von Standardvariablen zu definieren, wie zum Beispiel der Präsenz von Sicherheitssoftware und IAG-spezifischen Komponenten wie dem Attachment Wiper. Unterstützt komplexe Regeln für Endpunktrichtlinien mit flexibel anpassbaren Compliance-Prüfungen, bei denen Boolesche Operationen zum Einsatz kommen.

VERWALTBARKEIT

SSL VPN-Portal: Bietet einen zentralen Zugangspunkt (Single Access Point) für Anwendungen, unterstützt aber auch mehrere Zugangspunkte mit eigenen Richtlinienparametern, wie Partner-Extranets und Mitarbeiterportale, auf einem einzigen Gateway.

Umfassende Rahmenbedingungen für Richtlinien (Policy Framework):

- Standardeinstellungen für den Anwendungszugriff und Standardkonfigurationen für Endpunktrichtlinien (Endpoint Policies), um einen minimalen Integrationsaufwand und geringe laufende Verwaltungskosten sicherzustellen.
- Unterstützt das Intelligent Application Toolkit für die Definition von positiv logischen Regelsätzen, URL-Filter zur Ergänzung der Optimizer-Einstellungen und die Entwicklung von Richtlinien (Policies) für personalisierte oder proprietäre Anwendungen.
- Unterstützt das Intelligent Application Template, das die Rahmenbedingungen zur Entwicklung eines Application Optimizers sowohl für generische Web-Anwendungen als auch für komplexe Unternehmensanwendungen liefert, die Komponenten, Web-Parts und Objekte beinhalten.

Product	Celestix WSA3000	Celestix WSA4000	Celestix WSA6000	Celestix WSA8000	Celestix WSA8000h
					
System					
Form Factor	1U compact rack	1U compact rack	2U compact rack	2U compact rack	2U compact rack
Dimensions (WxDxH)	17.5" x 14.38" x 1.75"	17.5" x 14.38" x 1.75"	17.5" x 17.5" x 3.5"	17.5" x 19.75" x 3.5"	17.5" x 19.75" x 3.5"
Processor	Intel® Pentium Dual-Core	Intel Core 2 Duo	Dual-Core Intel Xeron	2 x Xeon Quad Core	2 x Xeon Quad Core
Front Bus Speed/Cache	800MHz/1MB	800MHz/21MB	1066MHz/4MB	1333MHz/12MB	1333MHz/12MB
Chipset Chipset	Intel 945GV	Intel 945GV	Intel 945GV	Intel 5100P	Intel 5100P
Memory (667MHz DDR2)	2GB	2GB	3GB	4GB	4GB
Hard Drive (SATA-II)	80GB	80GB	Hot swappable 3 x 80GB (RAID 5) + 1x 80GB hot spare	2 x 73GB SAS RAID 1	2 x 73GB SAS RAID 1
Disk Speed	7,200 rpm	7,200 rpm	7,200 rpm	15,000 rpm	15,000 rpm
LCD Panel	40x2 Character	40x2 Character	40x2 Character	40x2 Character	40x2 Character
Gigabit NICs (PCIe)	6	6	6	4	4
SSL Accelerator/HSM	nein/nein	ja/nein	ja/nein	ja/nein	ja/ja
Ports	2 x Serial Ports/Console 3 x USB 2.0 Ports	2 x Serial Ports/Console 3 x USB 2.0 Ports	2 x Serial Ports/Console 3 x USB 2.0 Ports	1 x Serial Ports/Console 3 x USB 2.0 Ports	1 x Serial Ports/Console 3 x USB 2.0 Ports
Power	300W Universal AC input 100V~240V 50/60Hz	300W Universal AC input 100V~240V 50/60Hz	300W Universal AC input 100V~240V 50/60Hz (redundant & hot swappable)	500W Universal AC input 100V~240V 50/60Hz (redundant & hot swappable)	500W Universal AC input 100V~240V 50/60Hz (redundant & hot swappable)
Appliance Software					
Microsoft IAG	3.7	3.7	3.7	3.7	3.7
Bundled User Licenses	10	10	10	10	10
Recommended max. users	<1,000	<2,500	<5,000	<15,000	<15,000
Recommended concurrent users	up to 500	up to 1,000	up to 2,500	up to 8,000	up to 8,000
Restore to factory default	ja	ja	ja	ja	ja
Restore to last known good version	ja	ja	ja	ja	ja
Update services	ja	ja	ja	ja	ja
Hardened OS	Embedded Windows Server 2003	Embedded Windows Server 2003	Embedded Windows Server 2003	Embedded Windows Server 2003	Embedded Windows Server 2003