

The logo for WSA (Web Security Appliance) is displayed in white text on a dark, rounded rectangular background.A photograph of the Celestix WSA SSL Appliance, a rack-mounted server device with various ports and a front panel display. The text "Celestix® WSA SSL Appliance" is overlaid at the bottom of the image.

## Celestix® WSA SSL Appliance

### 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 unternehmensinterner 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

The Celestix logo features the word "celestix" in a lowercase, sans-serif font, with a stylized orange arrow pointing upwards and to the right integrated into the letter 'x'.

## Umfassender 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 benutzerdefinierter Remote-Access-Policy (Fernzugriffsrichtlinie) umzusetzen.

## 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.

## Application Optimizer

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	✓	k.A.	✓	Upload/ Download	Teilweise positiv	✓
SharePoint Portal Server	✓	✓	✓	Upload/ Download/ Bearbeiten	Uneingeschränkt positiv logisch	✓
Domino Web Access	✓	k.A.	✓	Upload/ Download	Uneingeschränkt positiv logisch	✓
IBM WebSphere	✓	✓	✓	Upload/ Download/ Bearbeiten	Teilweise positiv	✓
SAP Portal	✓	✓	✓	Upload/ Download/ Bearbeiten	Nur negativ	✓
EMC Documentum Webtop	✓	✓	✓	Upload/ Download/ Bearbeiten	Teilweise positiv	✓
Dynamics	✓	k.A.	✓	Upload/ Download/ Bearbeiten/ Exportieren	Teilweise positiv	✓

## 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 kopplet 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 er sich durch die volle Unterstützung sämtlicher Winsock-Anwendungen aus – wie TCP und dynamische Ports.

### 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 Verbindung 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, Wartbarkeit 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	
<b>Benutzer</b>	Unterstützt eine unbegrenzte Benutzeranzahl auf einem einzigen Gateway.
<b>Hochverfügbarkeit</b>	Linear skalierbar auf bis zu 64 hochverfügbare Knotenkonfigurationen.
Verwaltbarkeit	
<b>Flexibilität</b>	Bietet standardmäßige Softwarekonfigurationen für alle gängigen Unternehmensanwendungen und individuelle Anpassungsmöglichkeiten, darunter Profile für die Authentifizierung, Autorisierung und Endpunkt-Compliance sowie kontextbezogene Web-Portale. Unterstützt positiv logische Regelsätze und URL-Filteranpassung und ermöglicht die Entwicklung von Regelsätzen für personalisierte oder proprietäre Anwendungen.
<b>SSL VPN-Portal</b>	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.
<b>Protokollierung und Berichterstellung</b>	Unterstützt die Überwachung, Protokollierung und Berichterstellung (Reporting) für das Verwaltungs- und Rechnungswesen auf Unternehmensebene (System, Benutzersicherheit und Session-Views): <ul style="list-style-type: none"> <li>• Der Event Monitor gewährleistet eine umfassende Ereignisüberwachung nach Benutzer, Anwendung und Zeitraum.</li> <li>• Der integrierte Event Logger protokolliert die Systemnutzung und Benutzeraktivitäten und sendet Warnmeldungen zu sicherheitsspezifischen Ereignissen an eine Verwaltungskonsole.</li> <li>• Das integrierte Event Query Tool bietet vorkonfigurierte Abfragemasken (Templates) und volle Reporting-Funktionalität.</li> </ul>
<b>Umfassende Rahmenbedingungen für Richtlinien (Policy Framework)</b>	<ul style="list-style-type: none"> <li>• Standardeinstellungen für den Anwendungszugriff und Standardkonfigurationen für Endpunktrichtlinien (Endpoint Policies), um einen minimalen Integrationsaufwand und geringe laufende Verwaltungskosten sicherzustellen.</li> <li>• 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.</li> <li>• 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.</li> </ul>
Zugriffsrichtlinie	
<b>Endpunkt-Compliance-Prüfungen</b>	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.

