

USP SECURE ENTRY SERVER™

TECHNISCHE INFORMATIONEN.

Sicherheit

- Filtert den HTML-Datenstrom und blockiert bekannte Angriffsszenarien (injection attacks, cross site scripting, buffer overflow etc.)
- Automatische Validierung von formularbasierten Benutzereingaben
- Verschlüsselung der URL und/oder Parameter
- Schutz vor Sessionsübernahme (session/cookie hijacking etc.)
- Automatisierte Transaktionssignatur
- Transparente Verschlüsselung von Anwendungs-Cookies
- Unterstützt beliebig viele physikalisch getrennte Netzwerkzonen
- Schützt Web-Services (SOAP/XML-Filter)

Verfügbarkeit/Performance

- Failover-Cluster
- Gewichtetes Load-Balancing der Anfragen auf die rückwärtigen Systeme
- Schutz vor DoS-Angriffen
- Transparente Datenkomprimierung für schnelleres Laden der Web-Seiten
- Beschleunigung von SSL-Verbindungen
- «Multi-Threaded»-Architektur sichert beste Performance auf modernen Prozessoren

Betriebliche Vorteile

- Konfigurationsdateien zentral verwaltbar
- Flexibles Monitoring und Reporting
- Administrationsportal für den direkten Zugriff auf das laufende System
- Einfache Wartbarkeit, z.B. durch Übertragung bestehender Sitzungen auf andere Systeme
- Bestehendes Know-how im Bereich Open Source kann weiterverwendet werden
- Unterstützt DMZ-Virtualisierung und -Konsolidierung
- Anbindung externer Filtersysteme über ICAP-Schnittstelle (z.B. Antiviren-Scanner)

Endbenutzervorteile

- Single Sign-On über alle Web-Applikationen
- Unterschiedliche Authentisierungsmethoden gleichzeitig nutzbar
- Einfache Integration zusätzlicher Anwendungen

- Schutz vor Datenverlust bei zeitaufwendigen Formularen durch speziellen Zwischenspeicher
- Eine Eintritts-URL für alle Web-Anwendungen

Compliance

- PCI DSS (Payment Card Industry Data Security Standard)
- ONR 17700 (sicherheitstechnische Anforderungen an Web-Applikationen)
- Audit Logs

Unterstützte Standards

- SSL v3 / TLS (RFC 4346)
- ICAP (RFC 3507)
- SAML 2.0
- HTTP 1.0/1.1 (inkl. «keep-alive»-Verbindung bis zum Backend)
- SOAP 1.1/1.2
- WSDL 1.1
- Web Application Firewall Evaluation Criteria 1.0
- Apache 2.2

Authentisierungsmethoden

- Zertifikatsbasiert (X.509 V3)
- RSA SecurID
- Aladdin eTokens
- NTLM (Single Sign-On innerhalb von Microsoft-Domänen)
- GSM SMS (Simple Messaging Service) OTP
- Benutzername/Passwort auf LDAP-Verzeichnisse (inkl. Microsoft Active Directory, Novell eDirectory, Siemens DirX, Sun Directory Server etc.)

Authentisierungssysteme

- RADIUS (RFC 2865), RSA ACE Server, Aladdin TMS, Microsoft-Domänencontroller

Betriebssysteme

- Sun Solaris 8/10 (Sparc)
- HP-UX 11iv23
- Linux (RHEL 5, SLES 10)
- TCSEC B1- und Common Criteria EAL4+-zertifizierte Systeme (Argus PitBull® Foundation)