



ProxyRA ist ein On Demand-SSL VPN und bietet Mitarbeitern, Partnern und Kunden einen sicheren Fernzugriff. ProxyRA verfügt über integrierte Endpunkt-Sicherheit und Funktionen zum Informationsschutz, VPN-Client-Software oder lokale Administratorenrechte sind nicht notwendig. So stellt ProxyRA die ideale Fernzugriffslösung für die Bereitstellung von Anwendungen und Ressourcen an unverwalteten Endpunkten dar, die außerhalb der Reichweite von IPSec VPNs und herkömmlichen SSL VPNs liegen. Proxy RA ist die erste verfügbare anwendungsunabhängige Architektur und nutzt die zum Patent angemeldete On Demand-Connector-Technologie.

FUNKTIONEN

On Demand-Fernzugriff

Umfassende Anwendungsunterstützung

- > Bietet standardmäßige Unterstützung von webbasierten und nicht-webbasierten TCP- und UDP-Anwendungen

Umfassende Unterstützung von Web-Anwendungen

- > Bietet störungsfreien kontinuierlichen Zugriff auf einfache, erweiterte und funktionsreiche Web-Anwendungen (XML, ActiveX, AJAX, Java etc.), ohne auf fehleranfällige URL-Umschreibung zurückgreifen zu müssen

Nur ein Zugriffsmodus für alle Benutzer

- > Der einzigartige On Demand-Konnektivitätsagent bietet On Demand-Zugriff auf Client/Server- und Web-Anwendungen

Unterstützung für gesperrte Umgebungen

- > Auf Benutzergeräten werden keine lokalen Administratorenrechte benötigt (einschließlich Macs und PCs mit dem erweiterten Sicherheitsmodell von Microsoft Vista)

Arbeiten wie vor Ort

- > Gewährt eine IPSec-ähnliche Benutzererfahrung (z.B. Starten von nativen Anwendungen über den Desktop)

Zugriff auf die Anwendungsschicht für alle Anwendungen

- > Kontrollierter Zugriff auf alle unterstützten Anwendungen, ohne dass uneingeschränkte Netzwerkschicht-Konnektivität erforderlich ist

Keine Änderungen am Desktop

- > Der Desktop wird nach Beendigung der Benutzersitzung so hinterlassen, wie er vorgefunden wurde (keine Systemänderungen oder Modifikationen); es wird keine Software zurückgelassen

Endpunktsicherheit

Integration mit SSL VPN

- > Endpunktsicherheit für verwaltete und unverwaltete Geräte ist nahtlos in den Fernzugriffs- und Verwaltungsfunktionen integriert

Scan-Durchführung vor der Authentifizierung und kontinuierlicher Scan nach Spyware

- > Die zum Patent angemeldete Technologie prüft vor der Anmeldung auf Keylogger und Framgrabber und scannt während der gesamten Benutzersitzung kontinuierlich nach Spyware

Automatische Unterdrückung von Spyware

- > Erkennt und unterdrückt Prozesse und Programme wie Framgrabber und Keylogger, die als potenzielle

Bedrohung eingestuft werden, für die gesamte Dauer der Benutzersitzung, ohne dass dabei dauerhafte Systemänderungen vorgenommen werden

On Demand-Host-Integritätsprüfung

- > Überprüfung verschiedener Bedingungen (wie persönliche Firewall-Einstellungen, Aktualisierungen von Antiviren-Software sowie Patches und Service Packs für Betriebssysteme) am Endpunkt

Personalisierbare Host-Prüfung

- > Granularer regelbasierter Zugriff - der Zugriff auf interne Ressourcen wird basierend auf dem Endpunkt-Sicherheitsstatus eingeschränkt

Bewertung von Client-Anwendungen

- > Über weiße und schwarze Listen wird durch Prüfsummenabgleich bestimmt, welche Anwendungen zugelassen werden

Anwendungsspezifischer Zugriff

- > Administratoren können bestimmen, welche Anwendungen auf bestimmte Ressourcen zugreifen dürfen und so verhindern, dass nicht-autorisierte Programme interne Daten abrufen

Konfigurierbares Split-Tunneling

- > Split Tunneling kann blockiert oder durchgeführt werden

Abgestimmte Anwendungs- & Benutzerverwaltung

Intuitive objektbasierte Regelverwaltung

- > Kontrolle des Benutzerzugriffs auf bestimmte Ressourcen durch problemlos zu verwaltende, objektbasierte Zugriffsregeln

Genauere Benutzer- und Zugriffskontrolle

- > Der Zugriff kann nach Benutzer, Zugriffsziel, Ursprung/Standort des Benutzers, Uhrzeit und Sicherheitsprofil des angeschlossenen Geräts definiert werden

Regelassistent

- > Mit dem benutzerfreundlichen Regelassistenten können Zugriffsregeln in kürzester Zeit erstellt werden

Umfassende Authentifizierungsunterstützung

- > Abgestimmt auf führende Authentifizierungssysteme wie Microsoft Active Directory, LDAP/LDAPS, RADIUS, RSA SecurID® und TACACS+

Spezielle Gruppen

- > Auf der Basis bestehender Verzeichnisgruppen oder von Benutzermerkmalen kann ein gezielter Zugriff auf bestimmte Ressourcen für spezielle Gruppen unterstützt werden

Flexibel abgestufte Zugriffskontrollen

- > Der Zugriff auf bestimmte Anwendungen oder Ressourcen unterliegt minimalen Sicherheitsstufen; dies gilt beispielsweise für Betriebssystem-Patches, Antiviren-Aktualisierungen oder persönliche Firewall-Einstellungen

Aktivitätsprotokolle mit flexiblem Such-Tool

- > Alle Aktivitäten von Benutzern und Anwendungen werden protokolliert, für die Suche nach bestimmten Einträgen steht ein intuitives Such-Tool zur Verfügung

System-Dashboard

- > Das Dashboard gibt einen Überblick über den Zustand des Systems (z.B. Prozessor- und Festplattenausnutzung), die gleichzeitig angemeldeten Benutzer und den allgemeinen Systemstatus

Individuelle Anmeldungsseite

- > IT-Administratoren können die Anmeldungsseite für Benutzer individuell gestalten, um beispielsweise die Unternehmensfarben, Corporate Branding und Corporate Messaging zu integrieren

Informationssicherheit

Integration mit SSL VPN

- > Informationssicherheit für verwaltete und unverwaltete Geräte, nahtlos in den Fernzugriff integriert

Browser-Sicherheit

- > Verschlüsselung aller vom Browser gespeicherten Informationen einschließlich der Cache-Dateien, temporären Dateien und Cookies. Nach Abschluss der SSL VPN-Sitzung werden sämtliche Sitzungsinformationen per DoD 5220.22-Spezifikation zur Datei Löschung beseitigt

Kontrolle der Informationsnutzung

- > Die weitere Nutzung von Informationen, auf die Benutzer über Web-Anwendungen zugegriffen oder die sie heruntergeladen haben, kann kontrolliert werden. Es ist beispielsweise möglich, für Dateien das Speichern, Drucken, Kopieren in die Zwischenablage, Ausschneiden und Einfügen sowie die Funktion "Bildschirmansicht drucken" zu erlauben oder zu blockieren

Schutz vor Framgrabbern und Keyloggern

- > Es wird nach Keyloggern und Framgrabbern gescannt. Erkannte Spyware wird neutralisiert, um den Diebstahl von persönlichen und unternehmensrelevanten Informationen zu verhindern

Skalierbarkeit und Leistungen

Flexible Benutzerkonfiguration

- > Unterstützung von 25 bis 5.000 gleichzeitigen Benutzern

Hochverfügbarkeit

- > Transparente automatische Ausfallsicherung für störungsfreie, ununterbrochene Konnektivität

Lastverteilung

- > Unterstützung externer Lastverteiler für die reibungslose Ausführung von leistungskritischen Anwendungen

Hochleistungsarchitektur

- > Problemlose Unterstützung von LAN-Geschwindigkeiten



RA510 SERIES		RA510-A	Technische Daten	
System				
Plattenlaufwerke	1x80 GB IDE		Abmessungen und Gewicht	
RAM	512 MB		Gehäuse	19 Zoll, rahmenmontierbar
Netzwerk-Schnittstellen	(2) integrierte (On Board) 10/100Base-T NICs mit Pass-Through		Abmessungen (L x B x H)	58 cm x 44 cm x 4,4 cm (22,8 in x 17,4 in x 2,7 in)
Optionale Karten	2x10/100/1000Base-T-Karte 2x10/100/1000Base-SX (Dual GigE Fibre)-Karte		Gewicht (maximal)	14,1 kg (31 lb)

Betriebsumgebung				
Stromversorgung	Wechselstrom 100-240 V, 50-60 Hz, 6,3-3,0 A			
Maximale Leistung	150 W			
Wärmeleistung	512 BTU/h			
Temperatur	5° C bis 35° C (41° F bis 95° F)			
Feuchtigkeit	Unter 90% relative Luftfeuchtigkeit, nicht kondensierend			
Höhe	Bis zu 3.048 m (10.000 ft)			

RA810 SERIES		RA810-A	RA810-B	Technische Daten	
System					
Plattenlaufwerke	73 GB SCSI	2x73 GB SCSI RAID	Abmessungen und Gewicht		
RAM	2 GB	3 GB	Gehäuse	19 Zoll, rahmenmontierbar	
Netzwerk-Schnittstellen	(2) integrierte (On Board) 10/100/1000 Base-T NICs		Abmessungen (L x B x H)	58 cm x 44 cm x 4,4 cm (22,8 in x 17,4 in x 1,7 in)	
Optionale Karten	2x10/100/1000Base-T-Karte 4x10/100/1000Base-T-Karte 2x10/100/1000Base-SX (Dual GigE Fibre)-Karte		Gewicht (maximal)	14,1 kg (31 lb)	14,7 kg (32,5 lb)

Betriebsumgebung					
Stromversorgung	Wechselstrom 100-240 V, 50-60 Hz, 6,3-3,0 A				
Maximale Leistung	375 W				
Wärmeleistung	1280,25 BTU/h				
Temperatur	5° C bis 35° C (41° F bis 95° F)				
Feuchtigkeit	Unter 90% relative Luftfeuchtigkeit, nicht kondensierend				
Höhe	Bis zu 3.048 m (10.000 ft)				

RA8100 SERIES		RA8100-A	Technische Daten	
System				
Plattenlaufwerke	2x73 GB SCSI RAID		Abmessungen und Gewicht	
RAM	4 GB RAM		Gehäuse	19 Zoll, rahmenmontierbar
Netzwerk-Schnittstellen	(2) integrierte (On Board) 10/100/1000 Base-T NICs		Abmessungen (L x B x H)	59,2 cm x 44,2 cm x 17,652 cm (23,3 in x 17,4 in x 6,95 in)
Optionale Karten	2x10/100/1000Base-T-Karte (Dual GigE) 4x10/100/1000Base-T-Karte (Quad GigE) 4x10/100/1000Base-SX (Quad GigE Fibre)-Karte		Gewicht (maximal)	24,8 kg (54,5 lb)

Betriebsumgebung				
Stromversorgung	Wechselstrom 100-240 V, 50-60 Hz, 65 W, 6,3-3,0 A			
Maximale Leistung	525 W			
Wärmeleistung	1.792 BTU/h			
Temperatur	5° C bis 35° C (41° F bis 95° F)			
Feuchtigkeit	Unter 90% relative Luftfeuchtigkeit, nicht kondensierend			
Höhe	Bis zu 3.048 m (10.000 ft)			

FÜR ALLE RA-SERIEN

Richtlinien	
Emissionen	FCC Klasse A, EN55022 Klasse A, VCCI Klasse A Nr.1706609, BSMI, CCC, C-tick
Sicherheit	CSA C22.2 Nr. 950 M95, UL 60950 3. Ausgabe, EN60950, TÜV-GS, TÜV-S, CCC, BSMI
Normen	UL/CSA, TÜV-S, BSMI, Ctick, CCC, CE
Support-Standardgarantie	90 Tage Software- & Telefon-Support, 1 Jahr Hardware-Support; erweiterte und aktualisierte Support-Pläne verfügbar.
Endbenutzer-Sprache	Englisch, traditionelles und vereinfachtes Chinesisch, Japanisch und Koreanisch
Protokolle & Anwendungen	SSL VPN unterstützt ICMP und praktisch jede TCP- oder UDP-Anwendung. Zu den getesteten Anwendungen und Protokollen gehören unter anderem HTTP; FTP; SMTP; RDP; VoIP; H.323; SIP; RTP/RTSP; Citrix ICA Client®; IIOP; Microsoft Outlook (Exchange, IMAP oder POP); PCanywhere®; Yahoo Messenger®, AOL Instant Messenger®, MSN Messenger Service®; Open Bloomberg®
Konnektivität und NAT	DNS-Proxying; Network Address Translation (NAT); Firewall und Proxy-Traversal
Leistung und Zuverlässigkeit	Hochverfügbarkeit, Unterstützung von externen Lastverteilern, Einzel-, Dual- und Quad-Prozessormodelle für höchste Leistung
Verwaltungstools	Webbasierte Verwaltungskonsolle, Echtzeit-Status und Monitoring, rollenbasierte Verwaltung
Audit und Protokollierung	Protokollierung von Sitzungen, Verbindungen und fehlgeschlagenen Verbindungen, Verwaltungs-Audit, Protokollierung von Sicherheitsereignissen am Endpunkt, Syslog-Unterstützung, Rotation von Log-Dateien und automatische Archivierung, redundante Protokollierung, Off-Gateway-Audit Trail
VPN-Zugangskontrollkriterien	IP-Adresse (Ursprung und Ziel); DNS-Domänenname; Anwendung/Port; Benutzer; Gruppe; Zeit; Host-Integritätsstatus
Verschlüsselungsstandards	AES mit 256-Bit-Verschlüsselung und SHA MAC; RC4 mit 128-Bit-Verschlüsselung und MD5 MAC; 3DES mit 168-Bit-Verschlüsselung und SHA MAC
Authentifizierungsmechanismen	Interner Benutzername & Kennwort (RFC1929); Microsoft Active Directory; LDAP/LDAPS; RADIUS; RSA SecurID®; TACACS+
Connector-Unterstützung	Microsoft Windows 2000 SP4+, Microsoft Windows XP SP1+, Microsoft Windows Vista, Internet Explorer 6 & 7; Apple Mac OS X 10.4+, Safari 2.0.4+

Blue Coat Systems, Inc. +49 89 360 36 750 Direkt • +49 89 360 36 700 Fax • www.bluecoat.com

Copyright © 2007 Blue Coat Systems, Inc. Alle Rechte weltweit vorbehalten. Dieses Dokument darf ohne die vorherige schriftliche Einwilligung von Blue Coat Systems, Inc. weder ganz noch teilweise reproduziert noch auf ein elektronisches Medium übertragen werden. Technische Daten können ohne vorherige Ankündigung geändert werden. Die in diesem Dokument enthaltenen

Informationen sind als genau und zuverlässig zu betrachten. Blue Coat Systems, Inc. übernimmt jedoch keinerlei Haftung für ihre Verwendung. Blue Coat ist in den Vereinigten Staaten und weltweit ein eingetragenes Markenzeichen von Blue Coat Systems, Inc. Alle anderen in diesem Dokument erwähnten Marken sind Eigentum ihrer jeweiligen Inhaber. vDS-RA-v2 1007