Für kleine und mittlere Unternehmen

Sicherheitslösungen der Serie SA 500 von Cisco

Sicherheitskomplettlösung für kleine und mittlere Unternehmen

Die Sicherheitslösungen der Serie SA 500 von Cisco®, Bestandteil der Cisco Small Business Pro Serie, sind umfassende Gateway-Sicherheitslösungen mit einer Kombination aus Firewall-, VPN- und optionalen E-Mail- und Internet-Sicherheitsfunktionen, die einen zuverlässigen Schutz Ihres Unternehmens bieten und einen Geschäftsbetrieb ohne Ausfallzeiten unterstützen. Diese benutzerfreundlichen Sicherheitslösungen ermöglichen Ihnen die Steuerung des Zugriffs auf Netzwerkressourcen, den Schutz der Unternehmensdaten sowie die Minimierung von Netzwerkausfällen. Die Produkte der Serie SA 500 von Cisco tragen außerdem zur Steigerung der Mitarbeiterproduktivität bei, indem sie eine Steuerung des Internetzugriffs ermöglichen, vor E-Mail-Spam, Phishing-Angriffen, unautorisierten Zugriffsversuchen und weiteren, neu entstehenden Bedrohungen schützen und zudem die Freisetzung von IT-Ressourcen bewirken, die andernfalls zur Virenbeseitigung und Systembereinigung eingesetzt werden müssten. Mit den Produkten der Serie SA 500 von Cisco können Sie neue Geschäftsanwendungen sicher implementieren, ohne dabei gefährliche Sicherheitslücken zu öffnen. Mobile Mitarbeiter und Geschäftspartner können zudem über das Internet unter Verwendung von IPsec- oder SSL-VPN-Services sicher mit Ihrem Netzwerk verbunden werden. Mit einer Lösung der Serie SA 500 von Cisco zum Schutz Ihres Netzwerks können Sie sich auf Ihr Kerngeschäft konzentrieren, ohne sich Sorgen über die neuesten Sicherheitsrisiken machen zu müssen.

Herausforderung

Das Internet ist für Unternehmen aller Größen zu einem unverzichtbaren Geschäftstool geworden. Es bietet zahlreiche neue Möglichkeiten zur Ausweitung der Geschäftstätigkeit und versetzt Partner und Telearbeiter in die Lage, über VPN-Verbindungen auf das Unternehmensnetzwerk zuzugreifen. Doch gleichzeitig ist es eine Schwachstelle, über die Unbefugte und Schadsoftware in Unternehmensnetze eindringen können, was sehr negative Folgen haben kann:

- Unbefugter Zugriff kann zum Verlust von Unternehmensdaten, ungeplanten Ausfallzeiten und damit verbundenen Haftungsproblemen führen.
- Viren können Systeme infizieren und deren Zusammenbruch sowie Betriebsunterbrechungen und Gewinnausfälle herbeiführen.
- Spam und Phishing sind lästige Störungen und können die Mitarbeiterproduktivität beeinträchtigen.
- Spyware ermöglicht Unbefugten Einblicke in Ihr Netzwerk und Ihre Daten und kann zum Diebstahl von Identitäten und zum Verlust von Unternehmensdaten führen.
- Das Aufrufen nicht geschäftsbezogener und bedenklicher Websites verringert die Produktivität und erhöht das Risiko von Viren- und Spyware-Angriffen sowie möglicher rechtlicher Probleme im Zusammenhang mit Mitarbeitern.

Lösung

Die Produkte der Serie SA 500 von Cisco bieten kleinen und mittleren Unternehmen ein umfassendes Maß an Gateway-Sicherheit und VPN-Konnektivität. Dank ihrer kombinierten Firewall-, E-Mail- und Internet-Sicherheitsfunktionen ermöglichen die Geräte der Serie SA 500 von Cisco die Abwehr von Bedrohungen, noch bevor diese ins Netzwerk eindringen und den Geschäftsbetrieb beeinträchtigen können. Die Geräte der Serie SA 500 von Cisco bieten folgende Vorteile:

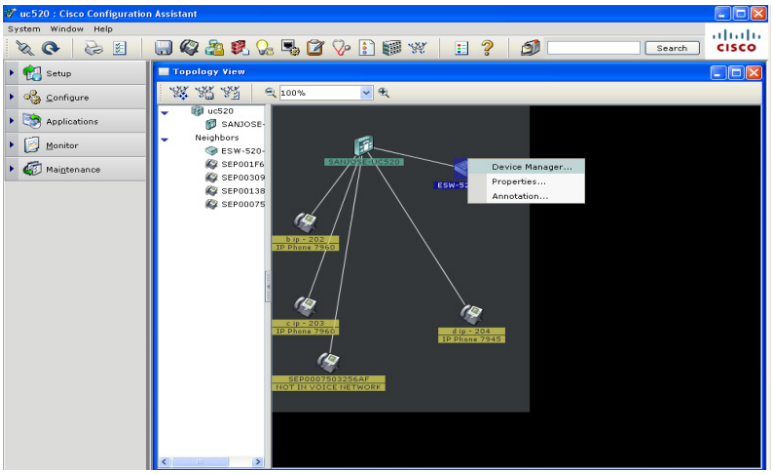
- **Sie gestatten den Fluss des regulären Unternehmensdatenverkehrs bei gleichzeitiger Blockierung unerwünschter Besucher.** Sie unterstützen zudem die Bereitstellung eines Netzwerkbereichs für den öffentlichen Zugriff, als DMZ (Demilitarized Zone) bekannt, zum sicheren Hosting von Datenservern, Webservern sowie anderen über das Internet zugänglichen Servern, ohne die internen LAN-Netzwerke des Unternehmens Sicherheitsbedrohungen auszusetzen.
- **Sie verhindern unberechtigten Zugriff und blockieren die gefährliche Peer-to-Peer-Kommunikation:** Mit der optionalen Intrusion Prevention System-Lizenz (IPS) für SA 500 kann die Serie SA 500 potenzielle Eindringversuche in das Unternehmensnetzwerk erkennen und die erforderlichen Maßnahmen ergreifen, um den Zugriff und weitere Gefahren zu verhindern. Darüber hinaus können die Geräte der Serie SA 500 Peer-to-Peer- und Instant Messaging-Datenverkehr blockieren und mithilfe von Protokollprüfungen die Netzwerksicherheit verbessern, die Mitarbeiterproduktivität erhöhen und die Verfügbarkeit des Netzwerks für den Unternehmensdatenverkehr gewährleisten.
- **Sie bieten uneingeschränkte E-Mail-und Internet-Sicherheitsfunktionen ohne Beeinträchtigung der Geschwindigkeit:** Die Geräte der Serie SA 500 von Cisco ermöglichen mit ihren stabilen Sicherheitsfunktionen zur Inhaltsüberwachung im Rahmen des optionalen Abonnements von Cisco ProtectLink Gateway die Bereitstellung entscheidender Sicherheitsservices zum umfassenden Perimeterschutz:
  - **Uneingeschränkter Schutz ohne Beeinträchtigung der Geschwindigkeit:** Die Bereitstellung der ProtectLink Gateway-Services erfolgt über einen speziellen Cloud-basierten Ansatz. An Ihr Unternehmen gerichtete E-Mails werden zunächst von Trend Micro, einem Technologiepartner von Cisco, unter Verwendung von Prüffunktionen der Enterprise-Klasse überprüft, um eine Reihe verschiedener Bedrohungen abzuwehren. So überprüft beispielsweise ProtectLink Gateway Ihre E-Mails auf mehr als 3 Millionen unterschiedliche Viren- und 400.000 Spywaremuster. Zudem wird über 10 verschiedene Prüftechnologien ein zusätzlicher Spam-Schutz bereitgestellt, in dessen Rahmen nicht nur die Reputation der Netzwerkadresse des Senders, sondern auch der tatsächliche Inhalt der E-Mail analysiert wird. Solche Merkmale werden Sie in anderen Produkten für kleine und mittlere Unternehmen vergeblich suchen. Neben den Sicherheitsvorteilen, die dieser Ansatz mit sich bringt, vermeidet er darüber hinaus den Kompromiss der Bandbreitenverringerung des Datenverkehrs, die bei vielen anderen Anbietern mit der Prüfung von E-Mail- und Internet-Inhalten einhergeht. Mit ProtectLink Gateway sind Sie in der Lage, die meisten Bedrohungen abzuwehren, noch ehe sie den Weg in Ihr Unternehmen finden, ohne dabei die Bandbreite zu beeinträchtigen.
  - **Antivirus:** Preisgekrönte Antivirus-Technologie schützt Ihre internen Netzwerkressourcen dort vor Angriffen durch bekannte und unbekannte Viren, wo dies am effektivsten ist: am Internet-Gateway. Das Filtern des E-Mail- und Internet-Verkehrs am Perimeter eliminiert die Notwendigkeit einer Ressourcen verschlingenden Beseitigung von Infektionen und erleichtert die Gewährleistung der Geschäftskontinuität.
  - **Antispyware**: Das Blockieren von Spyware am Gateway verhindert deren Eindringen in Ihr Netzwerk über den Internet-Datenverkehr (HTTP und FTP) und per E-Mail, wodurch kostspielige Verfahren zur Beseitigung von Spyware vermieden werden und die Produktivität der Mitarbeiter gesteigert wird.
  - **Antispam:** Das effektive Blockieren von Spam mit einer sehr geringen Zahl von Fehlalarmen erhöht die Effektivität der E-Mail-Kommunikation mit Kunden, Anbietern und Partnern.
  - **Antiphishing:** Der Schutz vor Identitätsdiebstahl dient der Abwehr von Phishing-Angriffen und verhindert so die unbeabsichtigte Preisgabe von Unternehmensdaten oder personenbezogenen Daten durch Mitarbeiter, was zu finanziellen Verlusten führen könnte.

- **URL-Filteroptionen:** Web- und URL-Filteroptionen können zur Steuerung der Internetnutzung der Mitarbeiter eingesetzt werden, indem der Zugriff auf unerwünschte oder nicht geschäftsbezogene Websites unterbunden wird. Auf diese Weise kann die Mitarbeiterproduktivität gesteigert und das Risiko gerichtlicher Schritte durch Mitarbeiter, die unangemessenen Webinhalten ausgesetzt wurden, begrenzt werden.

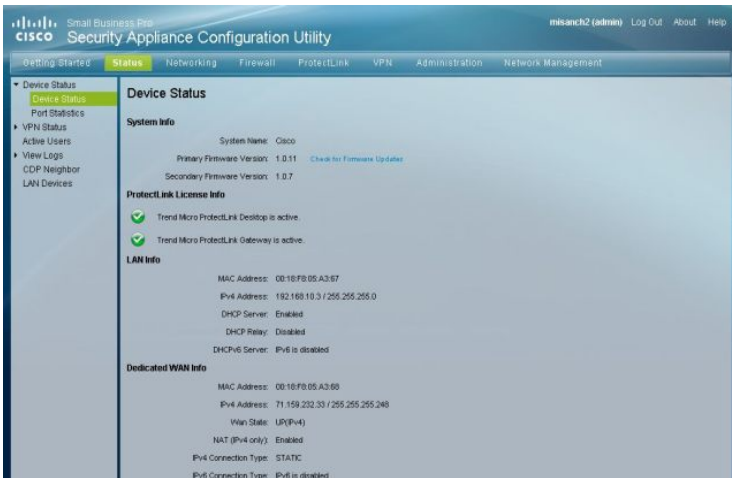
- **Erhöhung der Fernzugangssicherheit:** Im Rahmen der Unterstützung von VeriSign-VIP-Services (VeriSign Indentity Protection) bieten die Geräte der Serie SA 500 von Cisco Zwei-Faktor-Authentifizierung und Zugriffskontrolle über Einmalkennwörter zur Erhöhung der Fernzugangssicherheit, ohne den Erwerb zusätzlicher Authentifizierungsausrüstung erforderlich zu machen.
- **Einfache Implementierung und Verwaltung:** Die Geräte der Serie SA 500 von Cisco können mithilfe des integrierten browserbasierten Konfigurationsprogramms (Security Appliance Configuration Utility), einer leistungsstarken und benutzerfreundlichen Verwaltungs- und Überwachungsschnittstelle, verwaltet werden. Diese Lösung ermöglicht die umfassende Konfiguration und Überwachung aller Services innerhalb einer einzigen Anwendung. Das Security Appliance Configuration Utility-Programm kann auch über den Cisco Configuration Assistant gestartet werden. Zudem unterstützen die Geräte der Serie SA 500 von Cisco die Überwachung über Simple Network Management Protocol (SNMP).

In den Abbildungen 1 und 2 sind die Benutzeroberflächen des Cisco Configuration Assistant und des Security Appliance Configuration Utility-Programms dargestellt.

Abbildungen 1. Benutzeroberfläche des Cisco Configuration Assistant



Abbildungen 2. Benutzeroberfläche des Security Appliance Configuration Utility-Programms



Geschäftliche Vorteile

Die Sicherheitslösungen der Serie SA 500 von Cisco bieten Ihnen die erforderliche Sicherheit und Konnektivität, um folgende Ziele umzusetzen:

- **Bewältigung zunehmend komplexer Geschäftsanforderungen:** Implementieren Sie sicher neue Anwendungen dank der Bereitstellung erweiterter Sicherheitsservices auf Anwendungsebene für eine Vielzahl häufig genutzter Anwendungen wie webbasierte, E-Mail-, VoIP- (Voice over IP), Video- und Multimedia-Anwendungen.
- **Verbesserung der Authentifizierungssicherheit für Fernzugangsbenutzer:** Unterbinden Sie unbefugten Zugriff auf Ihr Unternehmensnetzwerk durch Verwendung von Hardware- oder Software-generierten Einmalkennwörtern.
- **Steigerung der Mitarbeiterproduktivität:** Verbessern Sie die Produktivität Ihrer Mitarbeiter durch Unterbindung von Spam, Spyware und unerwünschter Internetnutzung mithilfe des optionalen Cisco ProtectLink Gateway-Service.
- **Verbesserung der Ausfallsicherheit für Geschäftsabläufe:** Verhindern Sie Störungen unternehmenswichtiger Anwendungen und Services aufgrund von Sicherheitsverletzungen durch die Implementierung einer stabilen Firewall auf Unternehmensebene sowie die Unterstützung von E-Mail- und Web-Sicherheitsfunktionen.
- **Verringerung der IT-Kosten:** Setzen Sie IT-Support-Ressourcen frei, und vermeiden Sie kostspielige Verfahren zur Beseitigung von Problemen aufgrund von Spyware, Viren und anderer Malware, indem Sie dafür sorgen, dass diese gar nicht erst auftreten.
- **Bereitstellung eines einfach implementierbaren Fernzugangs:** Ermöglichen Sie Mitarbeitern und Partnern die schnelle und problemlose Verbindung mit dem SSL-VPN des Unternehmens.
- **Umsetzung einer hohen Betriebseffizienz:** Verringern Sie die mit der Implementierung und kontinuierlichen Verwaltung und Überwachung von Sicherheitslösungen verbundenen Kosten dank einer problemlos zu installierenden, benutzerfreundlichen Komplettlösung.
- **Verringerung des Haftpflichtrisikos:** Verringern Sie das Risiko von Haftpflichtforderungen gegenüber dem Unternehmen aufgrund von preisgegebenen Daten oder unangemessenen betrieblichen Sicherungsmechanismen durch die Implementierung umfassender Zugriffskontroll- und Gefahrenschutzservices im Rahmen einer Komplettlösung.
- **Beruhigende Sicherheit:** Ziehen Sie den maximalen Nutzen aus Ihrer Cisco Lösung durch Nutzung eines kostengünstigen Service-Angebots auf Abonnementbasis. Der Cisco Small Business Pro Service bietet Software-Upgrades und -Updates, einen erweiterten Zugriff auf das Cisco Small Business Support Center sowie Hardware-Ersatz am folgenden Geschäftstag.

Aufgrund all dieser Vorteile sind die Sicherheitslösungen der Serie SA 500 von Cisco die richtige Wahl, wenn es um Ihre Sicherheitsanforderungen und darum geht, Ihr Netzwerk und Ihre Mitarbeiter optimal für den Erfolg Ihres Unternehmens auszustatten.

Abbildung 3 zeigt eine Sicherheitslösung der Serie SA 500 von Cisco mit und ohne Drahtlosverbindungen.

Abbildungen 3. Sicherheitslösungen der Serie SA 500 von Cisco, SA 520W und SA 520

Technische Daten

Tabelle 1 enthält die technischen Daten zu den Geräten der Serie SA 500 von Cisco.

Tabelle 1. Modelle und technische Daten der Sicherheitslösungen der Serie SA 500 von Cisco

	SA 520	SA 520W	SA 540
Firewall			
Stateful Packet Inspection-Durchsatz*	200 Mbit/s	200 Mbit/s	300 Mbit/s
Firewall- plus E-Mail- und Internet-Sicherheitsdurchsatz*	200 Mbit/s	200 Mbit/s	300 Mbit/s
Verbindungen	15.000	15.000	40.000
Regeln	100	100	100
Zeitpläne	Ja	Ja	Ja
IPS	Ja	Ja	Ja
Peer-to-Peer- und Instant Messaging-Blockade	Ja	Ja	Ja
VPN			
Triple Data Encryption Standard (3DES)/Advanced Encryption Standard (AES) – VPN-Durchsatz*	65 Mbit/s	65 Mbit/s	85 Mbit/s
IPsec-VPN-Tunnel	Maximal 50	Maximal 50	Maximal 100
SSL-VPN-Tunnel	Umfasst 2 Plätze; zur Aufrüstung auf (max.) 25 Plätze Lizenz erforderlich	Umfasst 2 Plätze; zur Aufrüstung auf (max.) 25 Plätze Lizenz erforderlich	Umfasst (max.) 50 Plätze
Dead Peer Detection (DPD)	Ja	Ja	Ja
IPsec Network Address Translation (NAT) Traversal	Ja	Ja	Ja
NetBIOS-Broadcast über VPN	Ja	Ja	Ja
Cisco ProtectLink Gateway			
URL-Filterung	Mehr als 80 Kategorien	Mehr als 80 Kategorien	Mehr als 80 Kategorien
Schutz vor Bedrohungen aus dem Internet	Ja	Ja	Ja
Schutz vor Spam	Ja	Ja	Ja
Virensignaturen	Mehr als 3 Millionen	Mehr als 3 Millionen	Mehr als 3 Millionen
Spywaresignaturen	Mehr als 420.000	Mehr als 420.000	Mehr als 420.000
WLAN			
802.11b/g/n	Nein	Ja	Nein
2 x 3 MIMO (Multiple Input, Multiple Output)	Nein	Ja	Nein
2,4 GHz	Nein	Ja	Nein
Wi-Fi Multimedia (WMM) QoS	Nein	Ja	Nein
Unscheduled Automatic Power Save Delivery (U-APSD) (WMM Power Save [WMM-PS])	Nein	Ja	Nein

MAC-Filterung	Nein	Ja	Nein
Wired Equivalent Privacy (WEP), Wi-Fi Protected Access Pre-Shared Key (WPA2-PSK), WPA2-ENT	Nein	Ja	Nein
Basic Service Set Identifier (BSSID) oder virtuelle Zugangspunkte	Nein	Ja, 4 unterstützt	Nein
Übertragungsleistung dynamisch oder manuell einstellbar	Nein	Ja	Nein
Wi-Fi Protected Setup (WPS)	Nein	Ja	Nein
Sonstige			
Routing	Statisch, Routing Information Protocol (RIP) Version 1 und 2	Statisch, RIP Version 1 und 2	Statisch, RIP Version 1 und 2
VLANs	16	16	16
IPsec/Point-to-Point Tunneling Protocol (PPTP)/Layer 2 Tunneling Protocol (L2TP)-Durchleitung	Ja	Ja	Ja
Message Digest	MD5/SHA1/SHA2	MD5/SHA1/SHA2	MD5/SHA1/SHA2
Verschlüsselung	DES/3DES/AES	DES/3DES/AES	DES/3DES/AES
Benutzerdatenbank	100	100	400
Dynamischer DNS (DDNS)	Ja	Ja	Ja
Lastenausgleich	Ja	Ja	Ja
Integrierte und automatische Ausfallsicherung und Wiederherstellung	Ja, unter Verwendung eines optionalen Ports für Dual-WAN	Ja, unter Verwendung eines optionalen Ports für Dual-WAN	Ja, unter Verwendung eines optionalen Ports für Dual-WAN
VeriSign-VIP-Unterstützung	Ja	Ja	Ja
Physische Schnittstellen	• Alle Ethernet-Ports sind 10BASE-T-, 100BASE-TX-, 1000BASE-T-fähig • 4 LAN-Ports • 1 WAN-Port • 1 optionaler Port zur Verwendung als LAN, WAN oder DMZ-Port • 1 USB 2.0-Port • 1 Netzschalter	• Alle Ethernet-Ports sind 10BASE-T-, 100BASE-TX-, 1000BASE-T-fähig • 4 LAN-Ports • 1 WAN-Port • 1 optionaler Port zur Verwendung als LAN, WAN oder DMZ-Port • 1 USB 2.0-Port • 1 Netzschalter • 3 externe Antennen	• Alle Ethernet-Ports sind 10BASE-T-, 100BASE-TX-, 1000BASE-T-fähig • 8 LAN-Ports • 1 WAN-Port • 1 optionaler Port zur Verwendung als LAN, WAN oder DMZ-Port • 1 USB 2.0-Port • 1 Netzschalter
Umgebungstemperatur – Betrieb	0 bis 40 ºC (32 bis 104 ºF)	0 bis 40 ºC (32 bis 104 ºF)	0 bis 40 ºC (32 bis 104 ºF)
Lagertemperatur	–20 bis 70 °C (–4 bis 158 °F)	–20 bis 70 °C (–4 bis 158 °F)	–20 bis 70 °C (–4 bis 158 °F)
Internes Netzteil			
Spannungsbereich	90 bis 264 V, Wechselstrom, einphasig	90 bis 264 V, Wechselstrom, einphasig	90 bis 264 V, Wechselstrom, einphasig
Eingangsfrequenz	47 bis 63 Hz	47 bis 63 Hz	47 bis 63 Hz
Ausgangsspannungs-regelung	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V
Ausgangsstrom	Max. 2,5 A	Max. 2,5 A	Max. 2,5 A
Gehäusespezifikationen			
Format	1 HE, 19 Zoll- Rackmodell	1 HE, 19 Zoll- Rackmodell	1 HE, 19 Zoll- Rackmodell
Abmessungen (H x B x T)	1,73 x 12,12 x 7,08 Zoll (44 x 308 x 180 mm)	1,73 x 12,12 x 7,08 Zoll (44 x 308 x 180 mm) ohne Antennen	1,73 x 12,12 x 7,08 Zoll (44 x 308 x 180 mm)
Gewicht (mit internem Netzteil)	2,23 kg (4,91 lb)	2,34 kg (5,15 lb)	2,33 kg (5,14 lb)

* Leistungstestmethode: Maximale Leistung basierend auf RFC 2544. Bei allen Ergebnissen handelt es sich um bidirektionale Gesamtwerte. Die tatsächliche Leistung kann je nach Netzwerkumgebung und -konfiguration variieren.

Bestellung

In Tabelle 2 sind die Teilenummern der Sicherheitslösungen der Serie SA 500 von Cisco aufgelistet.

Tabelle 2. Produktteilenummern

Produkt	SKU
Sicherheitslösung SA 520	SA520-K9
Sicherheitslösung SA 520W	SA520W-K9
Sicherheitslösung SA 540	SA540-K9
ProtectLink Gateway mit unbeschränktem Internet + E-Mail für max. 25 Arbeitsplätze, 1-Jahres-Lizenz	L-PL-GW-25MAX-1=
ProtectLink Gateway mit unbeschränktem Internet + E-Mail für max. 25 Arbeitsplätze, 3-Jahres-Lizenz	L-PL-GW-25MAX-3=
ProtectLink Gateway mit unbeschränktem Internet + E-Mail für max. 100 Arbeitsplätze, 1-Jahres-Lizenz	L-PL-GW-100MAX-1=
ProtectLink Gateway mit unbeschränktem Internet + E-Mail für max. 100 Arbeitsplätze, 3-Jahres-Lizenz	L-PL-GW-100MAX-3=
IPS-Lizenz für Serie SA 500	L-SA500-IPS-1YR=
Cisco ProtectLink Endpoint, inkrementelle 5-Platz-Lizenz	L-PLEP-5=
Cisco ProtectLink Endpoint, inkrementelle 25-Platz-Lizenz	L-PLEP-25=
Cisco ProtectLink Endpoint, Verlängerung der inkrementellen 5-Platz-Lizenz	L-PLEP-5R=
Cisco ProtectLink Endpoint, Verlängerung der inkrementellen 25-Platz-Lizenz	L-PLEP-25R=
SSL-Lizenz für SA 520 und SA 520W	L-FL-SSL-SA520-K9=
Cisco Small Business Pro Service, 3 Jahre	CON-SBS-SVC2
SA 520 mit IPS und ProtectLink Web-Lizenzen, 3 Jahre	SA520-WEB-BUN3-K9
SA 520 mit IPS und ProtectLink Gateway, 25 Lizenzen, 3 Jahre	SA520-GW25-BUN3-K9
SA 520 mit IPS und ProtectLink Gateway, 100 Lizenzen, 3 Jahre	SA520-GW100BUN3-K9
SA 520W mit IPS und ProtectLink Web-Lizenzen, 3 Jahre	SA520W-WEB-BUN3-K9
SA 520W mit IPS und ProtectLink Gateway, 25 Lizenzen, 3 Jahre	SA520W-GW25BUN3-K9
SA 520W mit IPS und ProtectLink Gateway, 100 Lizenzen, 3 Jahre	SA520W-GW100BN3-K9
SA 540 mit IPS und ProtectLink Web-Lizenzen, 3 Jahre	SA540-WEB-BUN3-K9
SA 540 mit IPS und ProtectLink Gateway, 25 Lizenzen, 3 Jahre	SA540-GW25-BUN3-K9
SA 540 mit IPS und ProtectLink Gateway, 100 Lizenzen, 3 Jahre	SA540-GW100BUN3-K9

Sichere Verbindungen für Ihr Unternehmen

Das Netzwerk wird zunehmend zu einem zentralen Bestandteil der wichtigsten Geschäftsabläufe in Ihrem Unternehmen. Zur Gewährleistung des optimalen Geschäftsbetriebs und zur Bereitstellung eines Service, der den Erwartungen der Kunden entspricht, müssen Unternehmen über ein sicheres, leistungsfähiges und flexibles Netzwerk verfügen. Die Sicherheitslösungen der Serie SA 500 von Cisco vereinfachen die Kommunikation, indem sie die Kunden mit Ihrem Unternehmen und Ihre Mitarbeiter untereinander verbinden. Die Lösungen bieten die in diesem Zusammenhang für Unternehmen erforderliche hohe Sicherheit, sicheren VPN-Zugriff und erweiterte Routing-Services. Gleichzeitig unterstützen sie Sie bei Ihren Bestrebungen, die Kosten zu kontrollieren, verringern den Bedarf an separater Netzwerkausrüstung und vereinfachen die Netzwerkverwaltung. Ob Sie gerade eine kleines oder mittleres Unternehmen aufbauen oder ein bereits erfolgreiches Unternehmen erweitern – die Sicherheitslösungen der Serie SA 500 von Cisco können Ihnen die Aufgabe erleichtern, noch heute Ihr Verbindungsnetzwerk einzurichten – mit Raum für zukünftige Erweiterungen.

Service und Support

Die Sicherheitslösungen der Serie SA 500 von Cisco werden unterstützt durch den Cisco Small Business Pro Service zur kostengünstigen Absicherung Ihrer Investition, damit Sie sich beruhigt auf Ihr Kerngeschäft konzentrieren können. Dieser als Abonnement angebotene Service ermöglicht Ihnen, aus Ihren Produkten der Cisco Small Business Pro Serie den maximalen Nutzen zu ziehen. Der durch Cisco bereitgestellte, umfassende Service beinhaltet Software-Upgrades und -Updates, erweiterten Zugriff auf das Cisco Small Business Support Center und – falls erforderlich – Hardware-Ersatz am folgenden Geschäftstag. Er umfasst zudem einen Community-basierten Support, in dessen Rahmen kleine und mittlere Unternehmen Informationen austauschen und sich mithilfe von Online-Foren und Wikis gegenseitig dabei unterstützen können, ihre betriebliche Effizienz zu steigern, Risiken zu identifizieren und zu verringern sowie ihren Kundenservice zu verbessern.

Weiterführende Informationen

Weitere Informationen zu den Sicherheitslösungen der Serie SA 500 von Cisco finden Sie auf http://www.cisco.com/go/sa500, oder wenden Sie sich an Ihren lokalen Cisco-Händler.

Weitere Informationen zu den ProtectLink Gateway- und Endpoint-Produkten von Cisco finden Sie auf http://www.cisco.com/go/protectlink, oder wenden Sie sich an Ihren lokalen Cisco-Händler.

Weitere Informationen zum VeriSign-VIP-Produkt finden Sie auf http://www.cisco.com/go/viptoken, oder wenden Sie sich an Ihren lokalen Cisco-Händler.

Weitere Informationen zum Cisco Small Business Pro Service finden Sie auf http://www.cisco.com/go/proservice.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Gedruckt in den USA C78-542899-03 03/10

