8 Schritte zum perfekten Netzwerk Router Technik

Jo Kern – Systems Engineer - Partner Sales Group

Router für kleine Netze

- Internetzugang (NAT, DHCP) – Firewall
- VPN-Überblick und Vorteile
- IPSec- und SSL-VPN-Lösungen
- VPN-Konfiguration und -Implementierung
  - Gateway-to-Gateway
  - QuickVPN-IPSec-Client

Cisco Small Business Security Gateway Portfolio

Preis und Leistung

ASA 5500 Series & ISR 800 Series

Smartnet Support
High Availability
Zertifzierungen
Hoechstleistung
Enterpriseklasse

For Small Business

SA500
SRP500

RV042, RV082

RVS4000, WRVS4400N

RV120W, WRV210, RVL200

Unternehmen mit <100 PCs
Vielzahl von Security Features integriert
Trotzdem einfach zu konfigurieren
Auch Partner mit wenig Training können ein System aufbauen
Next Business Day Austausch mit Service Vertrag

Cisco Small Business

Wofür steht Cisco Small Business ?

- Zweckentwickelte Netzwerkprodukte mit dem Ziel der einfachen Installation und des Betriebs

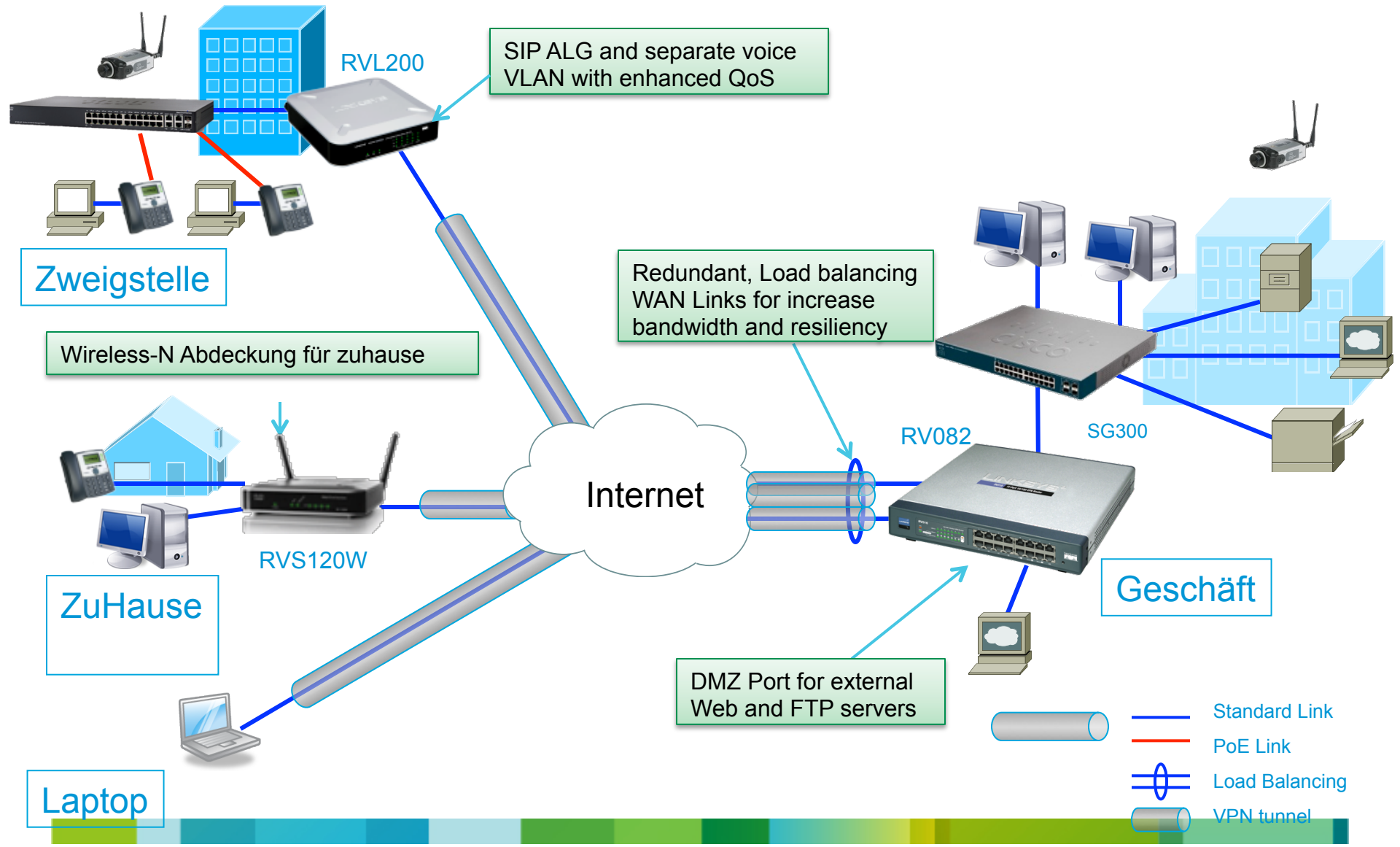
  Integrierte Web Server zur Konfiguration

  SNMP – Simple Network Management Protokoll

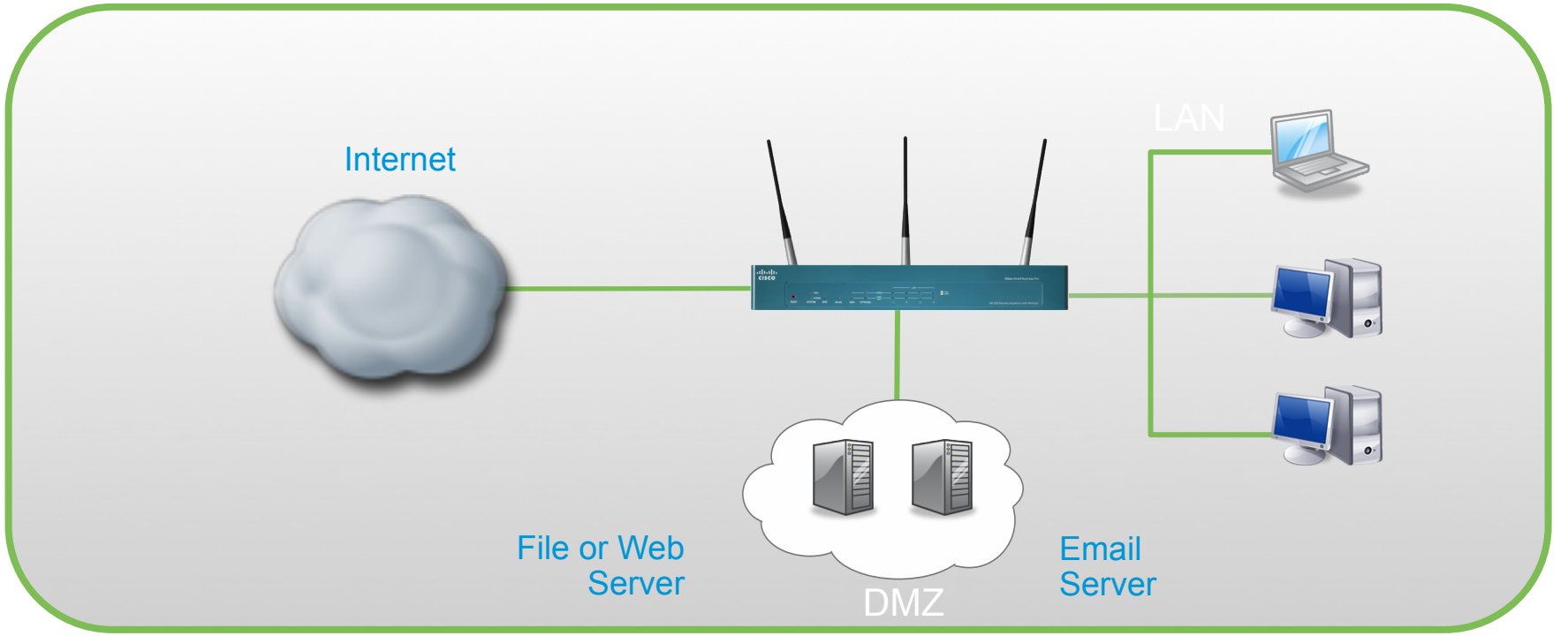
- Abstufung vom Einstiegs- bis Profimodell

  Abstufung erkenntlich in den ‘neuen’ Modellnamen 100, 200, 300, 500 Serie (noch nicht alle Modelle)

Cisco SB Router- Anwendungen

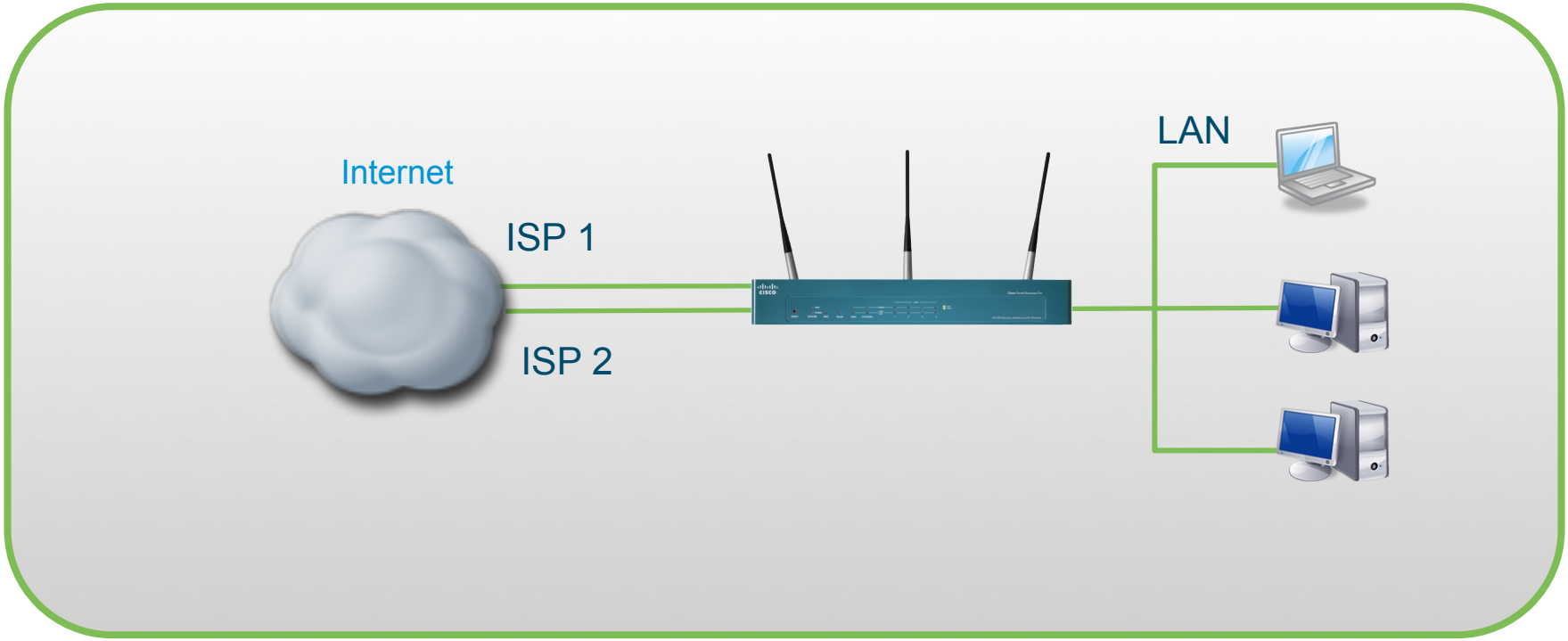


Business-Grade Firewall für das Small Business



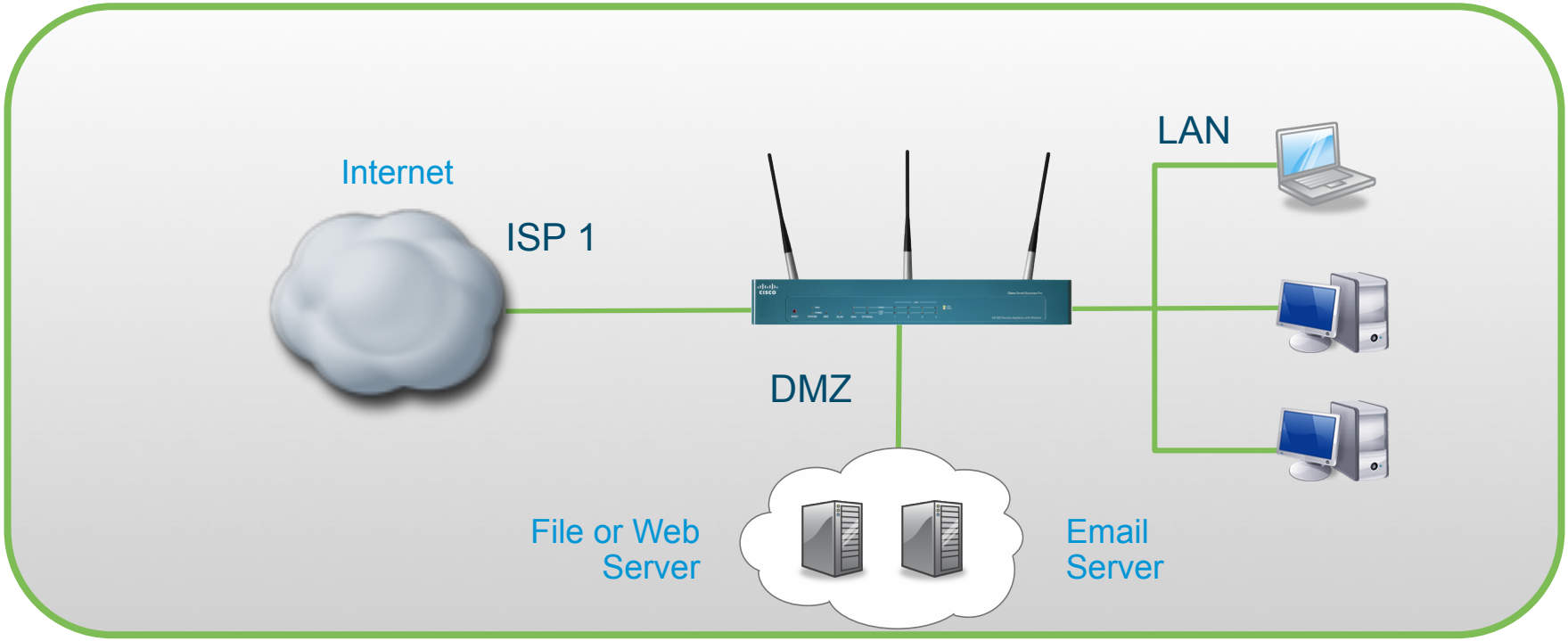
- **Firewall:** Schützt den Zugang in das LAN von aussen (Stateful).
- RVS4400, WRVS4400N, SA500: IPS schützt vor Angriffen im Datenverkehr
- SA500: Protectlink Endpoint Security: Lässt nur geschützte PCs in das Internet
- VPN: Erlaubt sicheren Zugang von aussen
- (Nicht 100er Serie) Email und Webfilter: Schützt dynamisch vor Viren über Email und Webseiten

Business-Grade Router für das Small Business



- **SA500, RV082, RV042:**
- **Dual WAN:** Zwei Anschlüße erhöhen die Verfügbarkeit (Backup und Loadsharing).

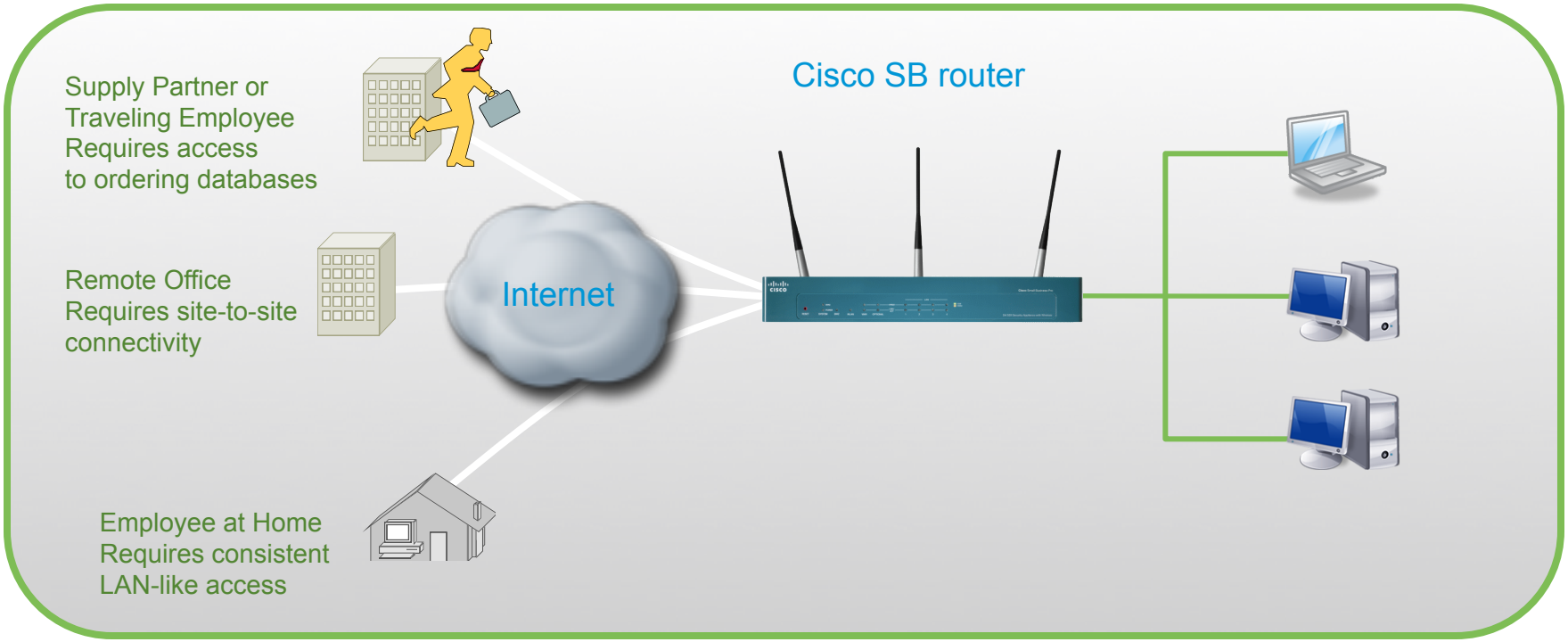
Business-Grade Router für das Small Business



- **SA500, RV082, RV042:**

- **Alternativ: Extra Port für DMZ:** Stellen sie Ihre öffentlichen Server sicher in das Netz.

VPN Zugang



- **Site-to-Site VPN:** Sichere Verbindung zwischen mehreren Standorten über das Internet.
- **Remote Access VPN:** Sicherer Zugang zum LAN über das Internet mittels IPSEC oder SSL VPN für Mitarbeiter und Partner.

RV 120W Features

- Firewall und Wireless Security
- IPsec VPN support with hardware acceleration (10 QVPN, 10 Ipsec)
- Standards-based 802.11n wireless access point, WDS
- Support for up to four separate, virtual networks
- 4-port 10/100 Mbps Fast Ethernet switch
- Deutsches Interface ab vorraussichtlich April
- VLANs, SNMP, IPV6

VPN Product Feature Matrix




	RVL200	WRV210	RVS4000	WRVS4400N
VPN Tunnels	5 SSL 1 IPSec	10 IPSec	5 IPSec	5 IPSec
Wireless & VLAN	Support up to 16 VLANs and 802.1q VLAN tagging (trunks)	802.11g Range Booster 5 VLANs 4 BSSIDs (MACs) Map SSID to VLAN	Up to 5 VLANs	Wireless-N Access Point – 802.11n(draft)

VPN Product Feature Matrix

	RV042	RV082
VPN Tunnels	50/50	50/100
Ethernet Ports	4 - 10/100 RJ-45 Ports	8 - 10/100 RJ-45 Ports
WAN Ports	1 10/100 RJ-45 Internet Port 1 10/100 RJ-45 DMZ/Internet Port WAN Port Balancing	1 10/100 RJ-45 Internet Port 1 10/100 RJ-45 DMZ/ Internet Port WAN Port Balancing
Management	Web, SNMP, and HTML Setup Wizards	Web, SNMP, and HTML Setup Wizards
Load Balancing	Supports dual WAN port Load Balancing	Supports dual WAN port Load Balancing

Der grosse Router Vergleich

http://www.cisco.com/en/US/products/ps9923/prod_models_comparison.html

Cisco Small Business Routers	RV 120W	RVL200	WRV210	RVS4000	WRVS4400N	RV042	RV082
WAN Ports	1 FE	1 FE	1 FE	1 GE	1 GE	2 FE	2 FE
Load Balancing	-	-	-	-	-	Yes	Yes
DMZ	Software-based	Software-based	Software-based	Software-based	Software-based	Port-based	Port-based
Lan Switch Ports	4 FE	4 FE	4 FE	4 GE	4 GE	4 FE	8 FE
VLAN Support	Yes	Yes	Port-based	Yes	Yes	-	Port-based
Wireless Access Point	b/g/n	-	b/g	-	b/g/n	-	-
WDS	Yes	-	Yes		Yes	-	-
IP Filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Port Filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPv6	Yes	-	-	Yes	Yes	-	-
RIP v1 / RIP v2	Yes / Yes	Yes / Yes	Yes / Yes	Yes / Yes	Yes / Yes	Yes / Yes	Yes / Yes
VLAN Routing	Yes	Yes	-	Yes	Yes	-	-
Quality of Service (QoS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SPI Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPsec DES / 3DES / AES	Yes/Yes/Yes	Yes/Yes/Yes	Yes/Yes/Yes	No/Yes/No	No/Yes/No	Yes/Yes/Yes	Yes/Yes/Yes
QuickVPN / Site-Site	10 \ 10	1 \ 1	5 \ 10	5 \ 5	5 \ 5	50 \ 50	50 \100
SSL VPN connections	-	5	-	-	-	-	-
Content/URL filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPS	-	-	-	Yes	Yes	-	-
Optionale Funktionen Support for Cisco ProtectLink Web	-	-	-	Yes	Yes	Yes	Yes

Cisco SB SRP 500

Service Ready Platform
WAN Termination

- WAN Termination
  with support of premium services
- Security, Wireless and Voice
- FastEthernet plus ADSL2+
- Especially designed for small business
- Standards-based provisioning
- Cost-effective and very competitively priced
- UMTS Modem support über USB Schnittstelle

Cisco SA 500 Serie Security Appliance

Model Number	Cisco® SA 520	Cisco® SA 520W	Cisco® SA 540
Firewall Performance	200 Mbps	200 Mbps	300 Mbps
VPN Performance	65 Mbps	65 Mbps	85 Mbps
Connections	15,000	15,000	40,000
Ports: LAN WAN Optional (for use as LAN, DMZ, or WAN redundancy or load balancing)	 4 1 1	 4 1 1	 8 1 1
Wireless (802.11 b/g/n	-	YES	-
IPsec VPN Tunnels	50 max.	50 max.	100 max.
SSL VPN Tunnels	2 seats included; license required to upgrade to 25 seats (maximum).		50 seats (max.) included
Email and Web Security (via Subscription)	Trend Micro ProtectLink Gateway with more than 3 million virus patterns, 420,000+ spyware patterns, and 80+ URL filtering categories.		

Cisco Protectlink Sicherheitsanwendung

- Wird extra verkauft
- RV042, RV082, SA500, WRVS4400N, RVS4000
- CiscoProtectLink Sicherheitslösungen

  Web Schutz: URL Filtering

  - blockiert URL auf der Basis von vom Benutzer ausgewählten Kategorien (Glücksspiele, OnlineAuktionen,...)
  - blockiert Web-Sites, die nicht sicher sind, automatisch

  Gatewayschutz: Web + E-mail-Scanning: blockiert SPAM, Viren, Phishing-Nachrichten

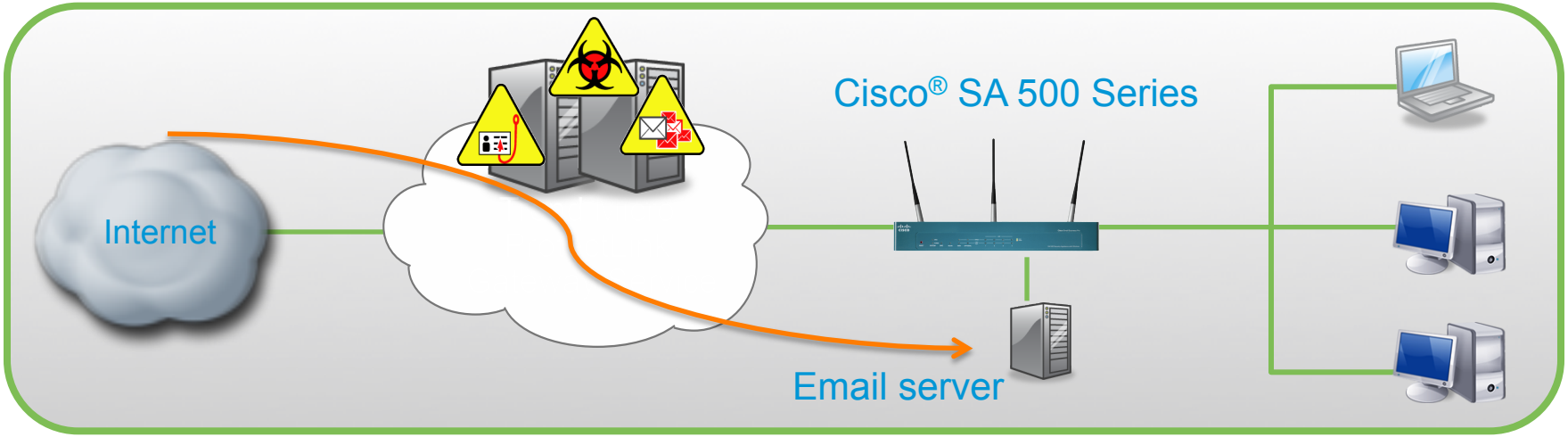
  E-mail Scanning und URL Filtering wird bei Trend Micro gemacht

  - Läuft auf dem Akamai Netzwerk
  - Schnelles Scanning, redundante Server
  - Anti-Virus Client mit Durchführung am Gateway

  Endpointschutz – Viren und Email Schutz im PC

- Services werden über die Web-Schnittstelle des Routers konfiguriert

Email Protection
via Trend Micro ProtectLink Gateway



- **Email Protection:** Emails sent to your businesses are scanned for spam, viruses, malware, spyware, and phishing attacks. Based on the award-winning Trend Micro Interscan Hosted Messaging Security (IMHS) offering.
- **Unique Cloud-Based Solution:**

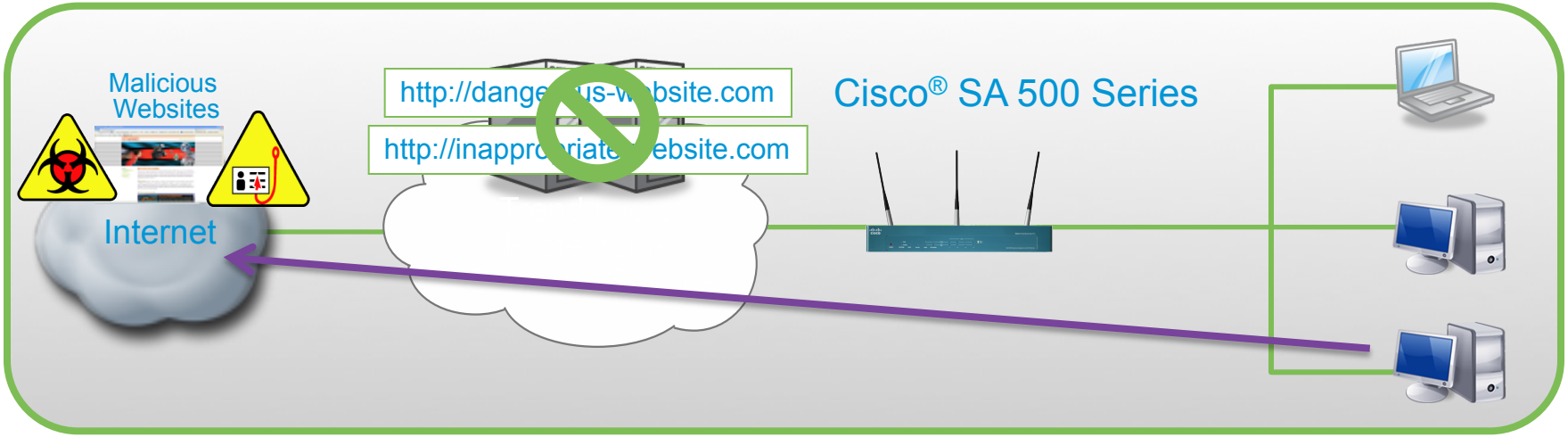
  Enables full-strength protection – over 3 million anti-virus patterns and over 400,000 anti-spyware patterns, 10 different techniques to ID spam, including methods that look at both the IP address of the sender and the actual content of the email itself.

  No risk of the inspection engines being out of date and unable to protect against the latest threats.

  Threats are stopped before they get to your business.

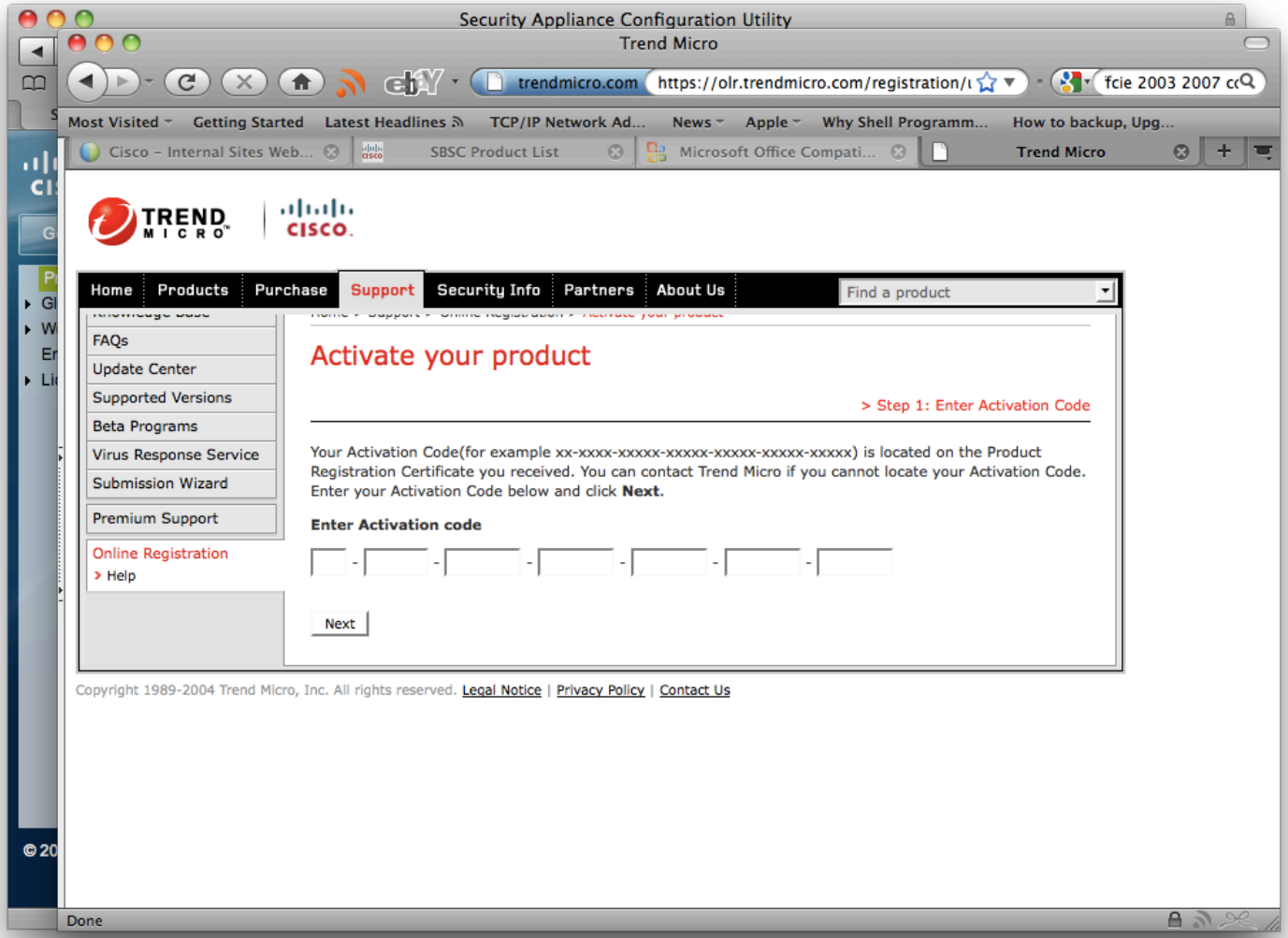
  Bandwidth is maintained even when security services are enabled.

Web Protection
via Trend Micro ProtectLink Gateway



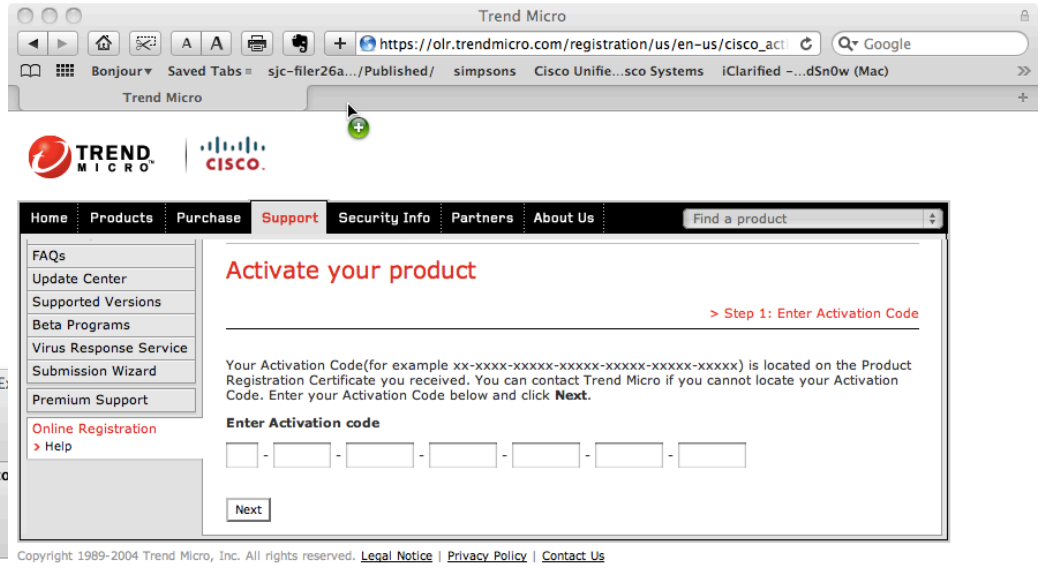
- **Web Threat Protection:** Reputation-based URL blocking prevents users from accessing dangerous websites known to have malware, phishing exploits, etc.
- **URL Filtering:** Over 80 categories of websites control employee web browsing and help increase employee productivity and reduce legal liability

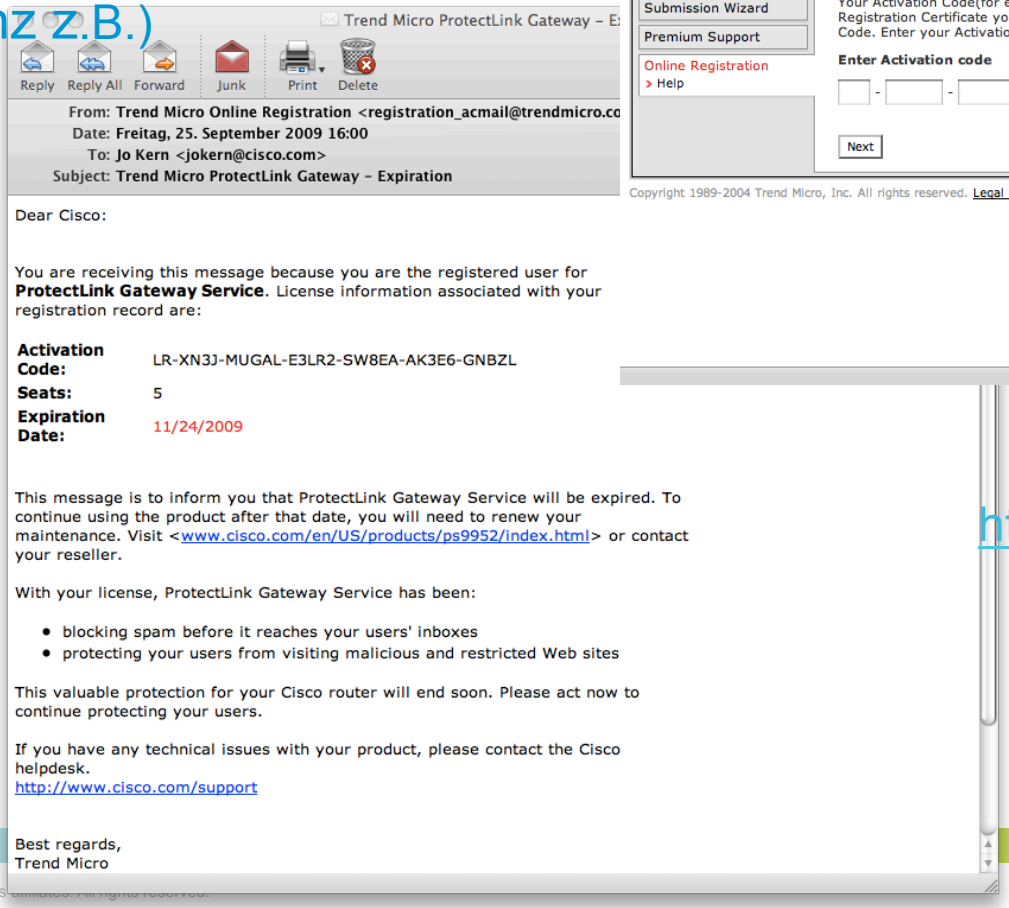
Protectlink Registrierung



Emails

- Verwaltung und Einrichtung des Dienstes über das Web
- Zusätzliche Infos über Emails (bei Ablauf der Lizenz z.B.)





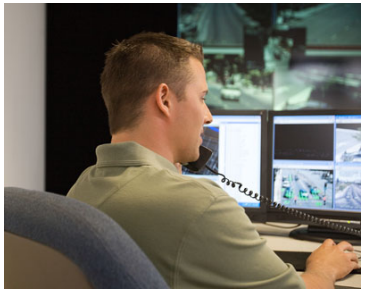
https://imhs.trendmicro.eu/loginPage.imss

VPN-Optionen: Gateway-to-Gateway-VPN mit IPSec

IPSec verschlüsselt den gesamten Datenverkehr und stellt so einen

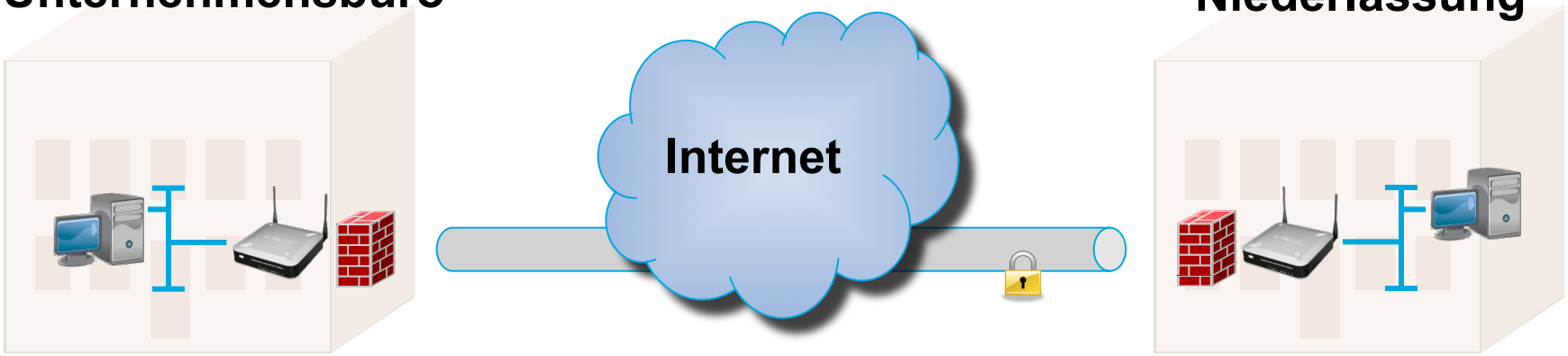
sicheren Tunnel zwischen den Standorten her.

- Gateway-to-Gateway-VPNs verbinden zwei oder mehr Standorte miteinander.
- Die sichere Tunnelverbindung steht immer zur Verfügung.



Unternehmensbüro

Niederlassung



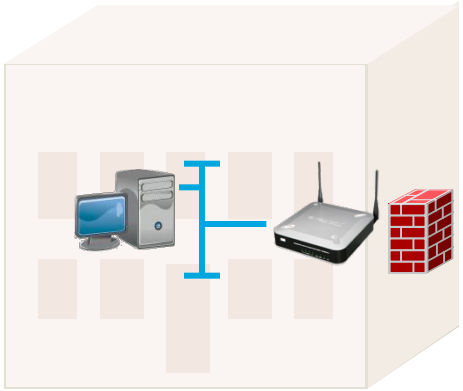
IPSec-Tunnel

VPN-Optionen: Client-to-Gateway-VPN mit IPSec

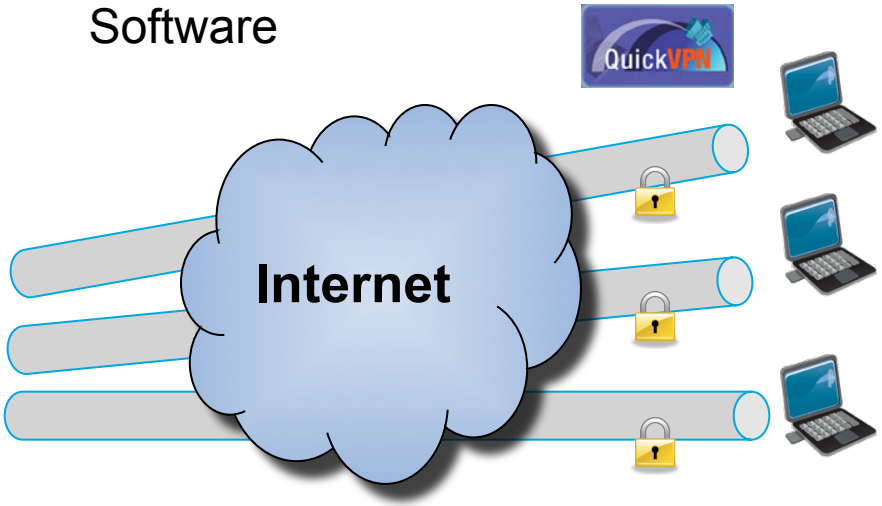
Für Client-to-Gateway-VPNs mit IPSec muss die Client-Software auf dem PC installiert sein.

- Client-to-Gateway-VPNs verbinden mobile Benutzer mit dem Unternehmensbüro.
- Die sichere Tunnelverbindung wird bei Bedarf eingerichtet.

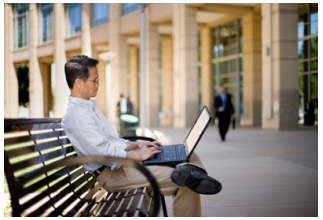
Unternehmensbüro



QuickVPN-Client-Software



Entfernte Mitarbeiter – zu Hause oder unterwegs



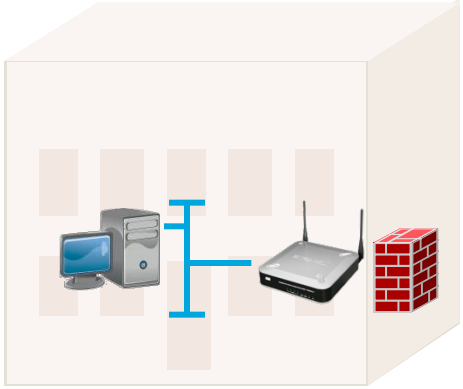
IPSec-Tunnel

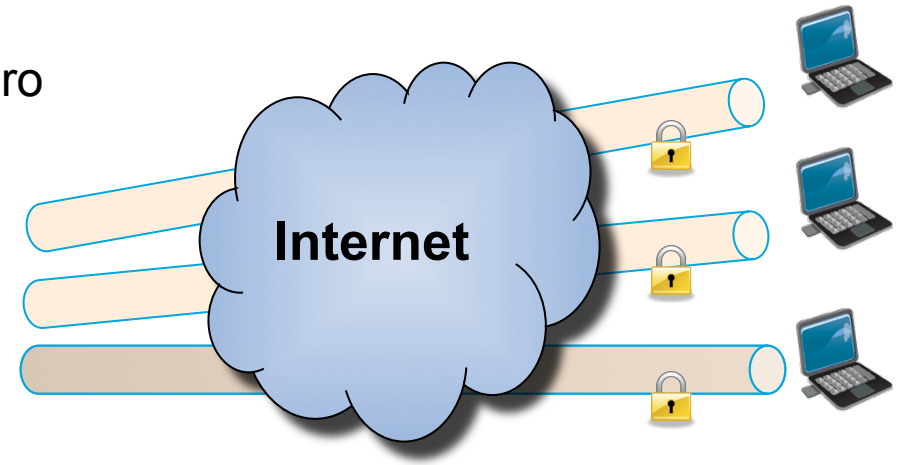
VPN-Optionen: Client-to-Gateway-VPN mit SSL

Client-to-Gateway-VPNs mit SSL verwenden einen Standard-Webbrowser für den Zugriff.

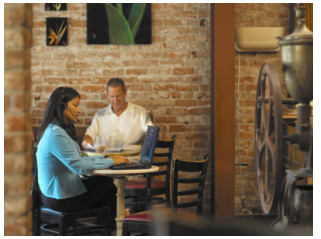
- Außendienstmitarbeiter können von jedem Computer aus eine sichere Verbindung herstellen.
- Ein Webbrowser stellt bei Bedarf eine sichere Tunnelverbindung her.

Unternehmensbüro





Entfernte Mitarbeiter, die einen Standard-Web-browser verwenden



SSL-Tunnel

SSL VPN Preferred for Remote Access

IPSec User

1. Create user account.
2. Send IPSec client to computer.
3. Install IPSec client.
4. Configure IPSec client.
5. User connects with VPN client.

(Conflicts likely if another brand of IPSec client is already installed.)

SSL VPN User

1. Create user account.
2. Send URL to user.

3. User connects to URL.

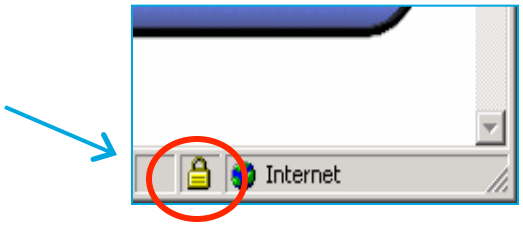
- **Easy Deployment:** SSL VPN sind schnell und einfach zu implementieren. Standard WWW Browser werden mitbenutzt.
- **Disaster Recovery:** Man erhält einen Zugang in das LAN, z.B. auch wenn man ungeplant nicht in das Büro kommen kann (Schnee)
- **Two-Factor Authentication:** VeriSign VIP service liefert einen hosted token-based authentication Dienst erweiterte Sicherheit der SSL Zugänge.
- **Licensed Feature**: Zusätzlich Lizenz erforderlich für den Cisco® SA520 and SA520W.

Was sind SSL-VPNs?

- SSL (Secure Sockets Layer)

  Endpunkte-Authentifizierung und Schutz privater Kommunikation durch PKI (Public Key Infrastructure)

  Die gleiche Technologie wird von sicheren Websites verwendet.



- Wie verwendet Cisco SSL für VPN?

  SSL wird zur Erstellung einer sicheren Verbindung zum RVL200, SA500 für die Authentifizierung verwendet.

  Nach der Authentifizierung wird eine virtuelle PPP-Sitzung über die SSL-Sitzung eingerichtet.

- Vorteile

  VPN über den Web-Browser → keine Client-Software

  Läuft transparent über Firewalls

  Zugriff von fast jedem Computer aus

VPN Konfiguration

IPsec Setup

Um die Daten zu verschluesseln muessen beide Seiten sich auf den Verschluesselungsstandard einigen. Dann muessen sie den gleichen Schluessel benutzen. Um die Schluesselauszutauschen gibt es 2 Methoden:

- Manuell
- Automatisch (IKE with Preshared Key, sichere asymmetrische Methode)

Verschlüsselungsalgorithmen

- **DES** – Data Encryption Standard (Daten-Verschlüsselungs-standard)
  - Wird heute als unsicher betrachtet, da er sehr anfällig für Brute-Force-Attacken ist.
  - Veröffentlichung 1977
  - Verschlüsselungsalgorithmus mit symmetrischem Schlüssel
  - Blockverschlüsselung: verwendet Datenblöcke von 64 Bit und einen Schlüsselwert von 56 Bit
- **3DES** – „Triple DES“ besser als DES aber langsam
  - Wurde wegen der Anfälligkeit von DES entwickelt
  - Veröffentlichung 1978
  - Verschlüsselungsalgorithmus mit symmetrischem Schlüssel
  - Blockverschlüsselung: verwendet Datenblöcke von 64 Bit und einen Schlüsselwert von 112 Bit effektiv
- **AES** – Advanced Encryption Standard (Erweiterter Daten-Verschlüsselungsstandard)
  - Wurde gründlich analysiert und wird heute weltweit eingesetzt
  - Veröffentlichung 1988
  - Verschlüsselungsalgorithmus mit symmetrischem Schlüssel
  - Blockverschlüsselung: verwendet Datenblöcke von 128 Bit und Schlüsselwerte von 128 Bit, 192 Bit oder 256 Bit

VPN Grundlagen

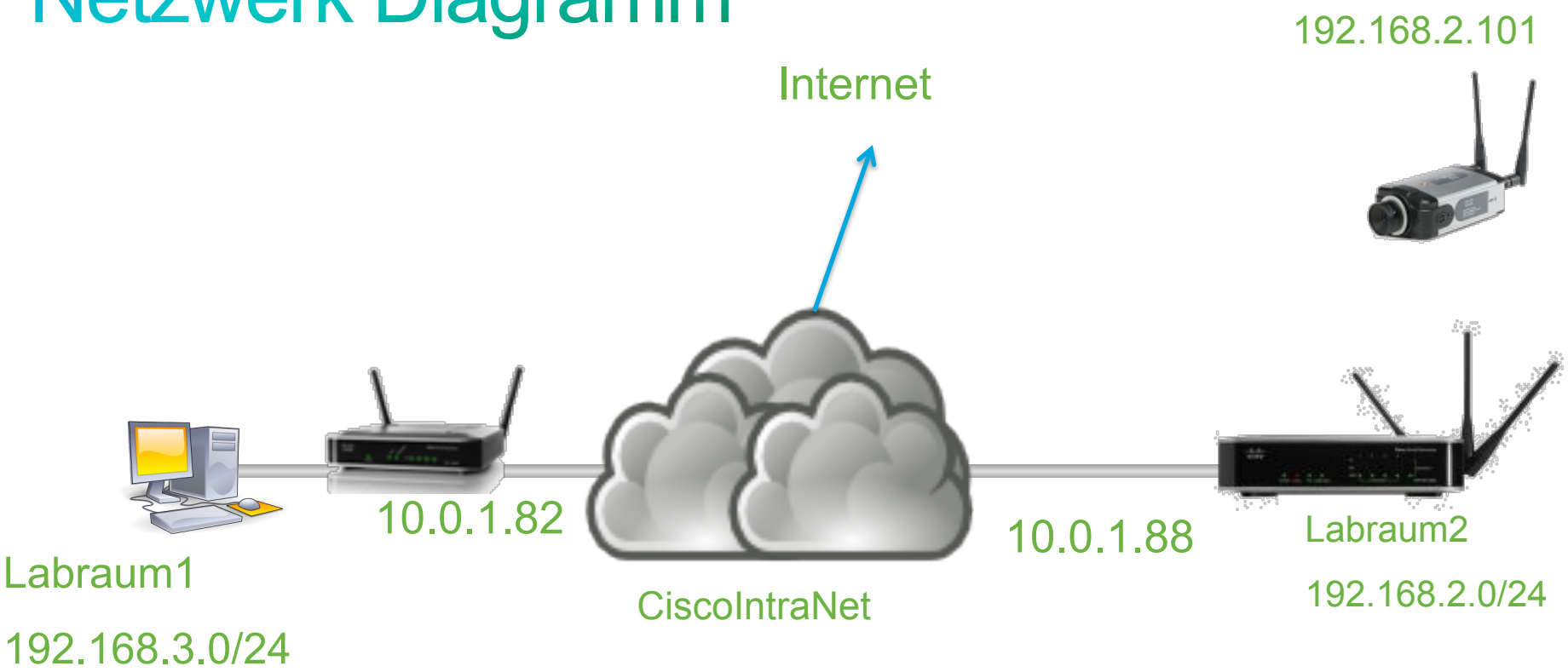
- Jede Seite muss ein eigenes IP Netzwerk sein (subnet). D.h. IP Adressen aus verschiedenen Adressbereichen haben
- Netz A: 192.168.2.0 / 255.255.255.0
- Netz B: 192.168.3.0 / 255.255.255.0
- Der Router hat normalerweiser die erste Adress aus dem Netzwerk, d.h 192.168.2.1.

Jeder Router muss auch mit dem Wissen ausgestattet werden, dass es das andere Netz gibt.

VPN Fundamentals

- Um einen VPN Tunnel herzustellen, muss man natuerlich die IP Adressen der Endpunkte kennen. Diese IP Adressen werden auch zur Identifizierung des Tunnels benutzt. Wenn die IP Adressen dynamisch vergeben werden, braucht man zusaetzliche Angaben zur Identifizierung.
- D.h. unterwegs habe ich einen Laptop und eine dynamische Ip Adresse, mein VPN client regelt das alles fuer mich.
- Wenn ich aber einen Router konfiguriere, dann muss ich noch zusaetzliche Angaben machen: domain name oder email adresse.
- Das dient zur Identifikation um des richtigen Tunnels. Zusaetzlich braucht man aber immer auch das Password (oder preshared key)

Netzwerk Diagramm

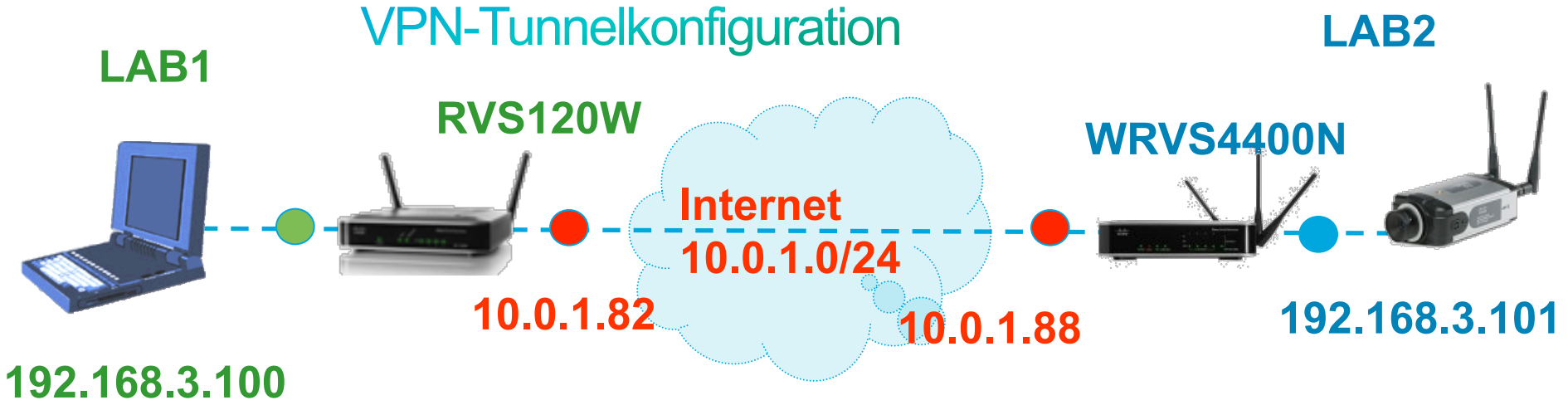


2 Optionen:

1.) Firewall Rules – Nachteil: Jeder kann zugreifen (ausser ich habe komplexe Firewall) – man könnte die Ueberwachung mitschneiden

2- VPN – sicherer verschluesselter Zugang

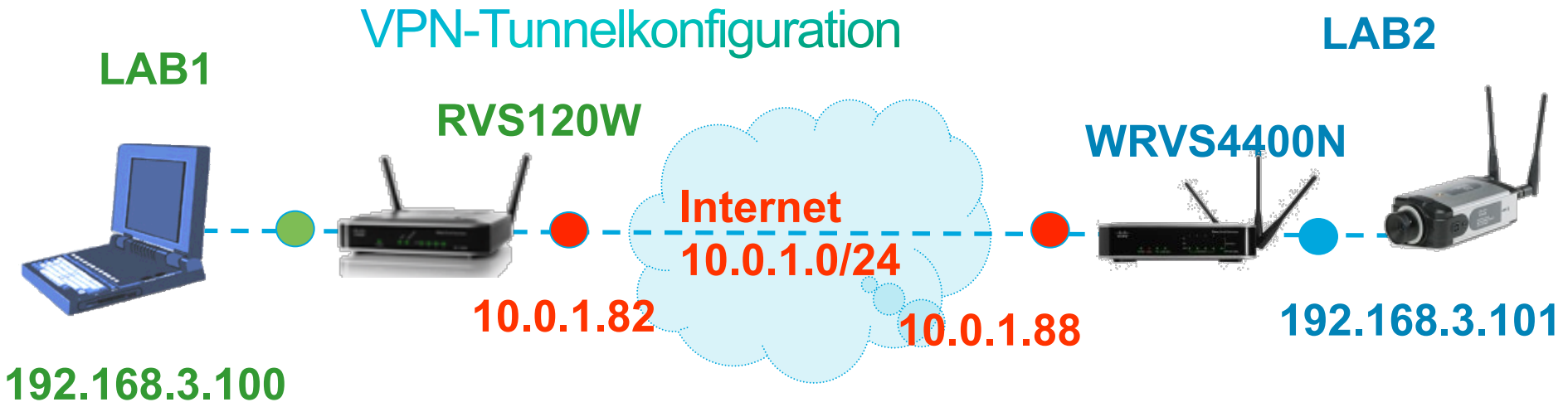
VPN-Tunnelkonfiguration



Alle VPN-Sicherheitsparameter müssen bei beiden VPN-Routern übereinstimmen. Wenn man unterschiedliche Hersteller verbindet muss man extra aufpassen, da die Parameter vielleicht anders benannt werden, oder an anderen Stellen konfiguriert werden

	RRVS120W	WRVS4400N
Verschlüsselung:	**3DES**	**3DES**
Authentifizierung:	**SHA1**	**SHA1**
Schlüsselmodus:	**IKE w/PSK**	**IKE w/PSK**
PFS:	**Aktiviert**	**Aktiviert**
Vorinstallierter SCHLÜSSEL:	**1234567890**	**1234567890**

VPN-Tunnelkonfiguration



Alle VPN-Sicherheitsparameter müssen bei beiden VPN-Routern übereinstimmen. Wenn man unterschiedliche Hersteller verbindet muss man extra aufpassen, da die Parameter vielleicht anders benannt werden, oder an anderen Stellen konfiguriert werden

Konfiguration des RV120W			
Lokale Sicherheits-IP oder Subnetz	Entferntes Sicherheits-Gateway	Lokale und entfernte sichere Gruppen-Typen	Entfernte sichere Gruppe
192.168.3.0	**10.0.1.88**	Subnetz	**192.168.2.0**

VPN-Unterstützung der Produkte anderer Hersteller

VPN-Produkte von Cisco SB unterstützen IPSEC die den gängigen Standards entsprechen.

Unterstützte Produkte anderer Hersteller:

- Win2000 VPN-Server
- Cisco 1720
- CheckPoint
- Nortel Contivity 1500
- SonicWall
- Nokia
- WatchGuard
- Sowie weitere Lösungen, die den gängigen Standards entsprechen

Designed to Enhance Partner Profitability

Enabling Partner Services

- Einfachste Installation mit Web GUI, Assistent und Voreinstellungen

Zusätzlicher Umsatz

SSL VPN licenses for remote access

– SA 520 & SA 520W come with 2 seats. License increases seat count to 25 users, the maximum.

– SA 540 comes with 50 seats. No license required.

- Cisco ProtectLink Gateway

– Web and Email, Endpoint Sicherheit in verschiedenen

–http://www.cisco.com/web/DE/portal/produkte-loesungen/sec

–Small Business Service

3 Jakhre Support mit NBD Austausch fuer UVP USD

Cisco Small Business Pro Service

“3 Jahre Sorglos Paket”

$19	$69	$149	$499
CON-SBS-SVC1	CON-SBS-SVC2	CON-SBS-SVC3	CON-SBS-SVC4
			
SPA525G	SA500	SR520 T1	UC540

- Software Updates for Bug Fixes
- Next Business Day Hardware Replacement (D,A,CH)
- Extended Access to Small Business Support Center
- Access to Small Business Support Community
- Online Chat Support

Distributoren

Comstor Networks, a Westcon Group company
Kaiserin-Augusta-Allee 113
10553 Berlin
Tel: 030/3 46 03-300
Fax: 030/3 46 03-399
Ansprechpartner:
Comstor Sales Team
Email: sales@comstor.de

Vertrieb der Cisco Small Business Reihe (ehemals Linksys by Cisco Business-Reihe). Kein Vertrieb von weiteren Cisco Lösungen.
Actebis Peacock GmbH
Lange Wende 43
59494 Soest
Ansprechpartner: Sven Schmidt
E-Mail: sschmidt@actebispeacock.de
Tel: 0 29 21/99-28 75
Fax: 0 29 21/99-36 59
cisco.actebis.com

INGRAM MICRO
INGRAM MICRO Distribution GmbH
Heisenbergbogen 3
85609 Dornach b. München
Telefon: 089 / 4208-2760
Telefax: 089 / 4208-2750
E-mail: sales-cisco@ingrammicro.de
Cisco SMB Portal bei Ingram Micro:
www.ingrammicro.de/cisco
Ansprechpartner:
Cisco Product Management Team
Cisco Fokus Sales Team

Tech Data GmbH & Co. OHG
Geschäftsbereich Azlan
Kistlerhofstraße 75
81379 München
Zentrale: +49 89 4700 -5520
Zentrale Fax: +49 89 4700 -5312
Cisco SMB Portal bei TD Azlan:
www.techdata.de/cisco
Ansprechpartner:
Cisco Business Unit