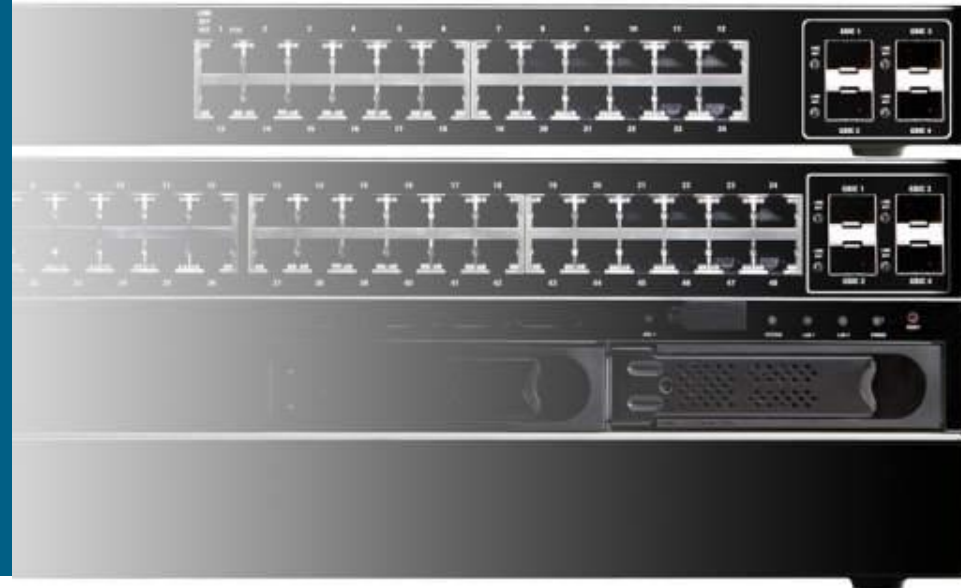




IDEA2.0 SBBU
Przełączniki
część praktyczna

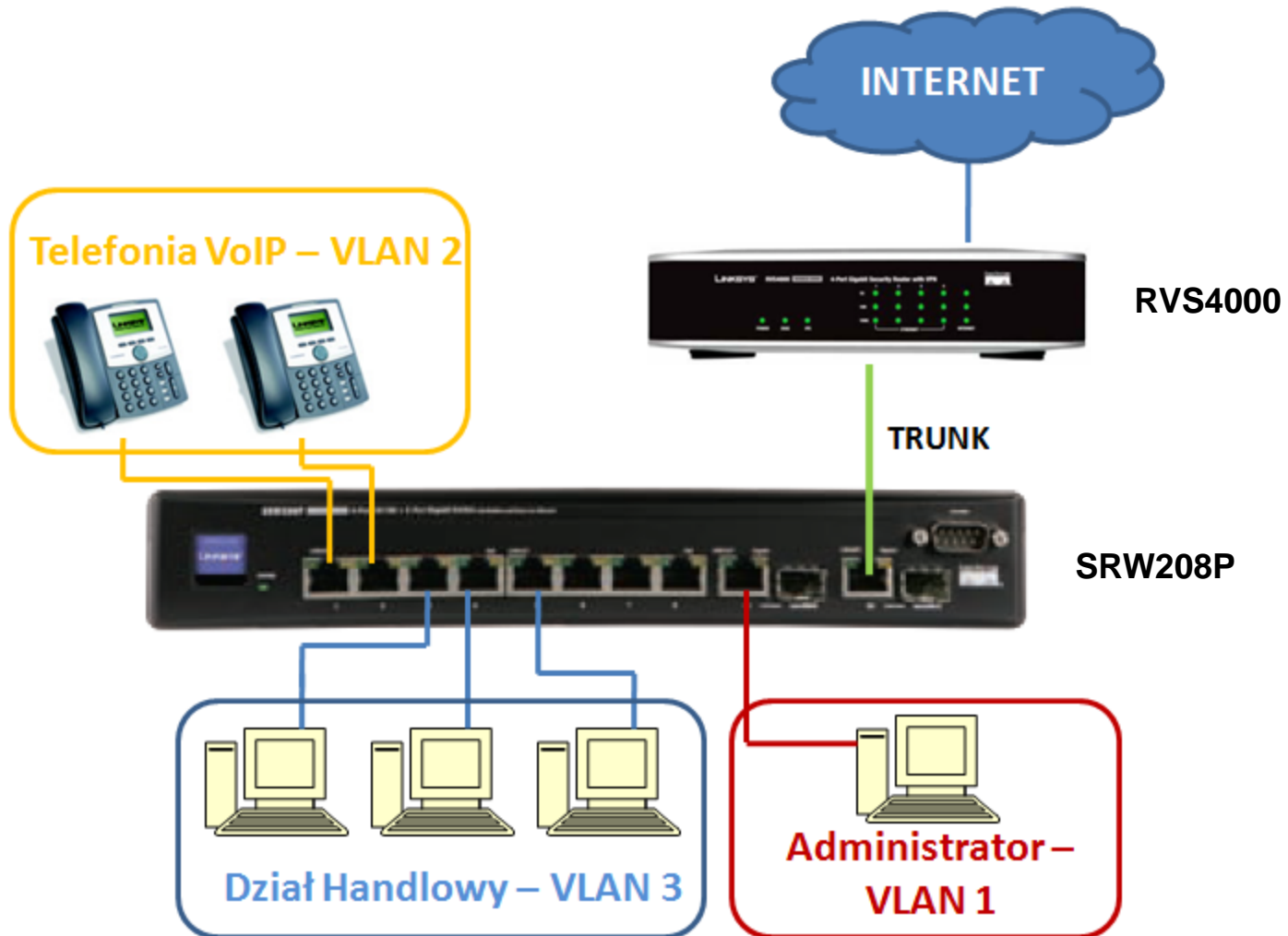


Paweł Latała, Cisco Systems Poland
Łukasz Naumowicz, Konsorcjum FEN

Agenda

- Topologia
- Administracja przełącznikami z rodziny SRW
- Wirtualne sieci prywatne VLAN
- Podstawy QoS

Topologia



Administracja

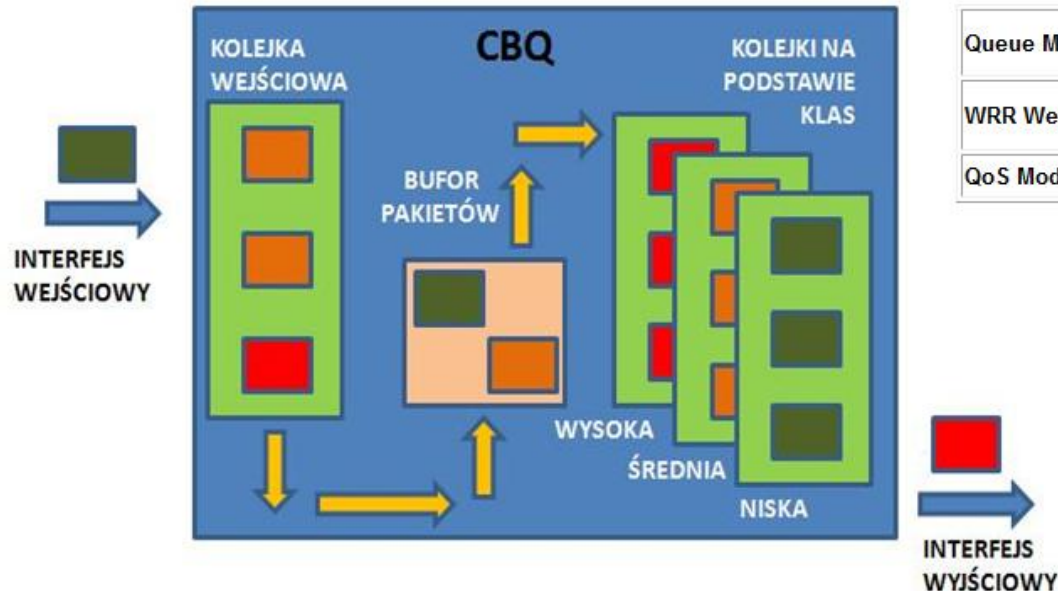
- Zmiana hasła
- Ustawienie danych charakterystycznych: lokalizacja
- Ustawienie adresu IP
- Kopiowanie plików konfiguracyjnych
- Dwie metody konfiguracji www lub LCLI

Wirtualne sieci prywatne VLAN

- Tworzenie VLANów
- Opis trybów portów i przypisanie portu do VLANu
- Łącza typu trunk
- Konfiguracja od strony przełącznika - SRW208P
- Konfiguracja od strony routera - RVS4000

Podstawy Quality of Service

- Opis mechanizmu
- Określenie trybu podstawowy/zaawansowany
- Nadawanie priorytetów dla portów

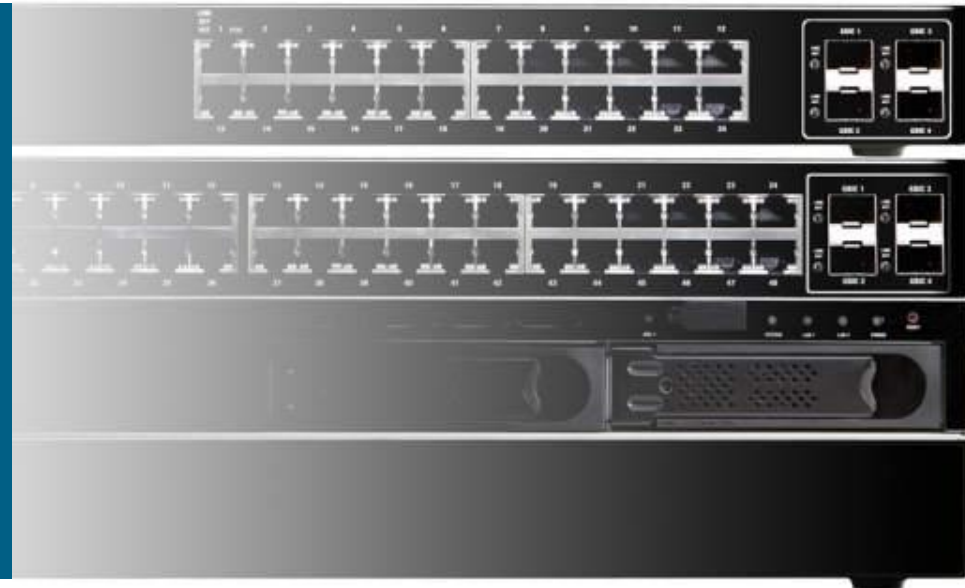


Queue Mode	<input type="radio"/> Strict Priority <input checked="" type="radio"/> WRR <small>WRR is not supported in Jumbo Frame mode.</small>
WRR Weight	<input type="text" value="1:2:3:4"/> <small>The ratio of Low/Normal/Medium/High queue</small>
QoS Mode	Port Based ▾

Port-Based Settings	
1	high ▾
2	high ▾
3	high ▾
4	high ▾
5	high ▾
6	high ▾
7	high ▾
8	high ▾



IDEA2.0 SBBU Routery i sieci bezprzewodowe



Paweł Latała, Cisco Systems Poland
Łukasz Naumowicz, Konsorcjum FEN

Agenda

- Routery/bramy VPN
- Biznesowe punkty dostępowe
- Przykłady konfiguracji
- Q&A

Routery

- Obsługa połączeń VPN – IPSec i SSL (wybrane modele)
=> Bezpieczna komunikacja pomiędzy oddziałami firmy i zdalnymi pracownikami (telepraca)
- Bezpieczeństwo: Firewall i ochrona przed atakami DoS, filtracja portów
- Łatwa instalacja i zarządzanie, SNMP, interfejs www, opcje monitorowania stanu urządzenia itd.
- Dostępne modele ze zintegrowanym punktem dostępowym – idealne dla mniejszych instalacji
- Telepraca => WRV200/210 jest idealnym routerem dla pracowników zdalnych



Routerzy VPN

Dwa porty WAN



RV016
UWAGA – niedostępny w Polsce



RV082



RV042

Pojedynczy port WAN



RVS4000



RVL200

- Zintegrowany firewall SPI
- Zintegrowany moduł IPS/IDS (tylko RVS4000)
- Sprzętowy akcelerator szyfrowania dla połączeń VPN
 - Wydzielony port DMZ (tylko RV0XX)
- Obsługa połączeń SSL VPN (tylko RVL200)
- Trend Micro Protectlink email and filtering



Routery VPN ze zintegrowanym punktem dostępowym

802.11g MIMO



WRV210



WRV200

802.11n MIMO / Gigabit WAN



WRVS4400N

- Do 10 tuneli IPSec VPN(5 w WRVS4400N)
 - Zintegrowany firewall SPI
 - Obsługa wielu SSID (tylko WRV2xx)
 - Zintegrowany IPS/IDS (tylko WRVS4400N)
 - Anteny dookólne
- Trend Micro Protectlink email and filtering - od H1CY09



Prostota Quick VPN

Wprowadź nazwę użytkownika i hasło

Wyeksportuj certyfikat dla klientów i administratora

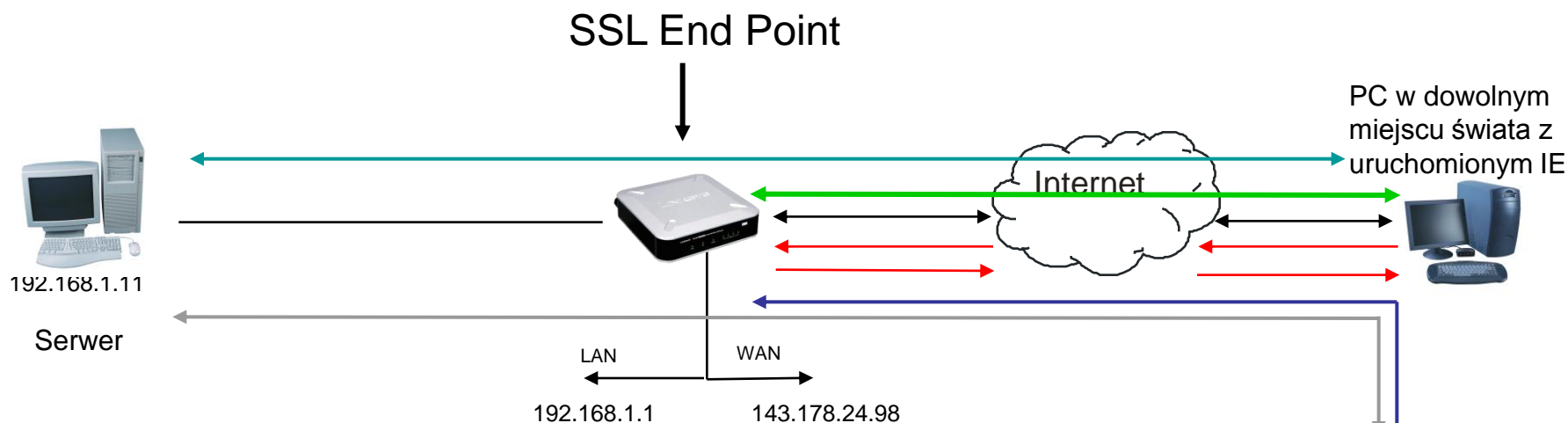
Zapisz certyfikat QuickVPN w katalogach na komputerach klientów

Uruchom oprogramowanie Linksys QuickVPN Client

Wprowadź adres bramy zdalnej nazwę użytkownika



Połączenia SSL VPN



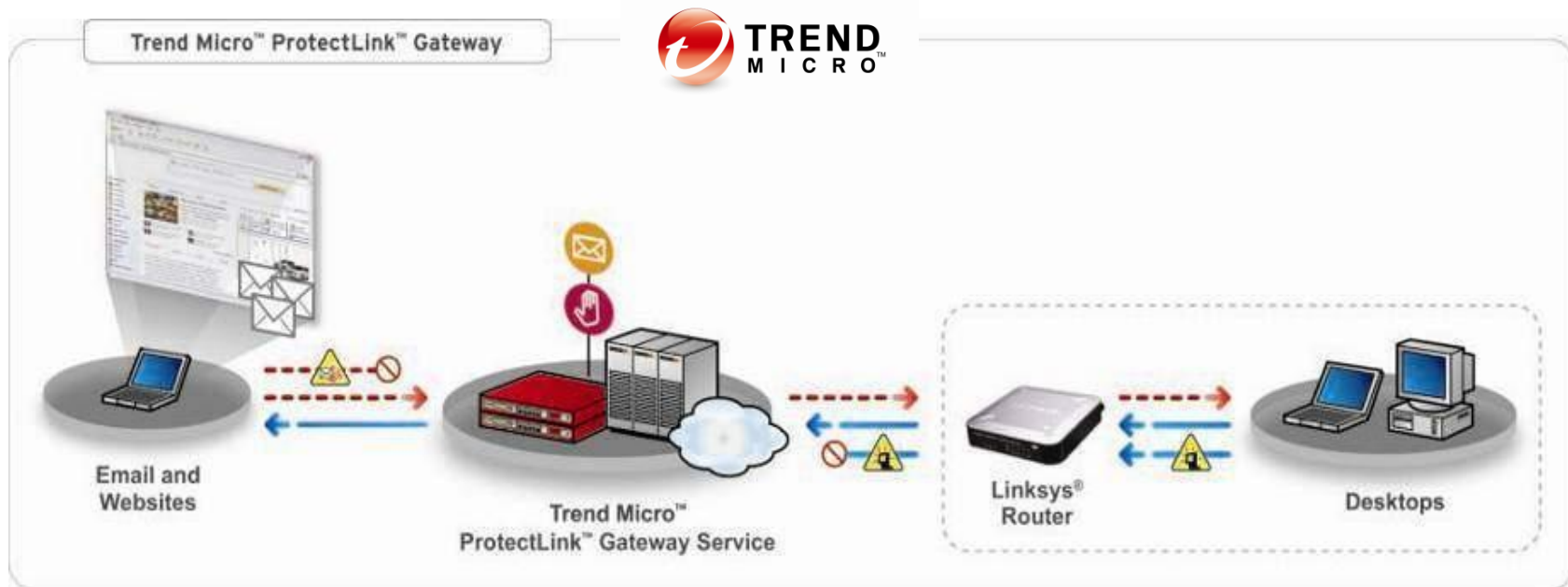
1. Klient uruchamia przeglądarkę i wpisuje adres https gateway'a SSL VPN
2. Łączenie i negocjacja parametrów połączenia
3. Zestawienie tunelu SSL pomiędzy komputerem klienta i routerem SSL
4. Bezpieczny i łatwy dostęp do zasobów sieciowych
5. + 1 tunel IPSec do połączenia z centralą firmy umożliwiający bezpieczny dostęp dla serwera z oddziału

Centrala firmy

Jak działa ProtectLink Gateway

• Trend Micro ProtectLink Gateway

- ProtectLink Gateway: Chroni pocztę elektroniczną oraz ruch www
 - Blokowanie spamu oraz filtracja adresów URL bazująca na reputacji stron internetowych
 - Usługa hostowana – Nie ma konieczności instalacji żadnego nowego sprzętu czy oprogramowania




Ograniczenie dostępu do www

ProtectLink

[System Summary](#)
[Setup](#)
[DHCP](#)
[System Management](#)
[Port Management](#)
[Firewall](#)
[ProtectLink](#)
[VPN](#)
[Log](#)
[Wizard](#)
[Support](#)
[Logout](#)

Web Protection
Email Protection | License

Web Protection



Enable URL Filtering
 Enable Web Reputation

URL Filtering

Filter selected categories
Reset Counters

URL Categories	Filtering		
	Business Hours	Leisure Hours	Instances Blocked
<input checked="" type="checkbox"/> Adult	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
<input type="checkbox"/> Business	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Computers/Bandwidth	<input type="checkbox"/>	<input type="checkbox"/>	0
<input type="checkbox"/> Computers/Harmful	<input type="checkbox"/>	<input type="checkbox"/>	0
<input type="checkbox"/> Computers/Communication	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> General	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Social	<input type="checkbox"/>	<input type="checkbox"/>	0

Business Hour Setting

Business Days:

Sun
 Mon
 Tue
 Wed
 Thu
 Fri
 Sat

Business Times:

All day (24 hours)
 Specify business hours

Note: Time not designated as business time will be considered leisure time.

Morning
 Afternoon

From: 08:00 To: 12:00
 From: 12:00 To: 17:00

Web Reputation

Security level:

High Blocks a greater number of Web threats but increases the risk of false positives.
 Medium Blocks most Web threats and does not create too many false positives. This is the recommended setting.
 Low Blocks fewer Web threats but reduces the risk of false positives.

SITEMAP

Web Protection manages and protects employee Internet use by blocking access to non-work-related and malicious Web sites. [More...](#)

Ograniczenie dostępu do www

Approved URLs

URLs in this list will always be accessible.

Enable Approved URLs list

URLs to approve:

Add >>

Approved URLs list	(Max. 20 URLs)
cisco.com	
linksys.com	
fen.pl	
www.tlenofon.pl	

Example:
'xxx.com' matches 'xxx.com'
and all the URLs that
begin with 'xxx.com/'
(Separate multiple entries with semicolons)

Approved Clients

Specify the client IP addresses or IP ranges to exclude from the URL filtering rules:

Enable Approved Clients list

IP addresses/range:

Add >>

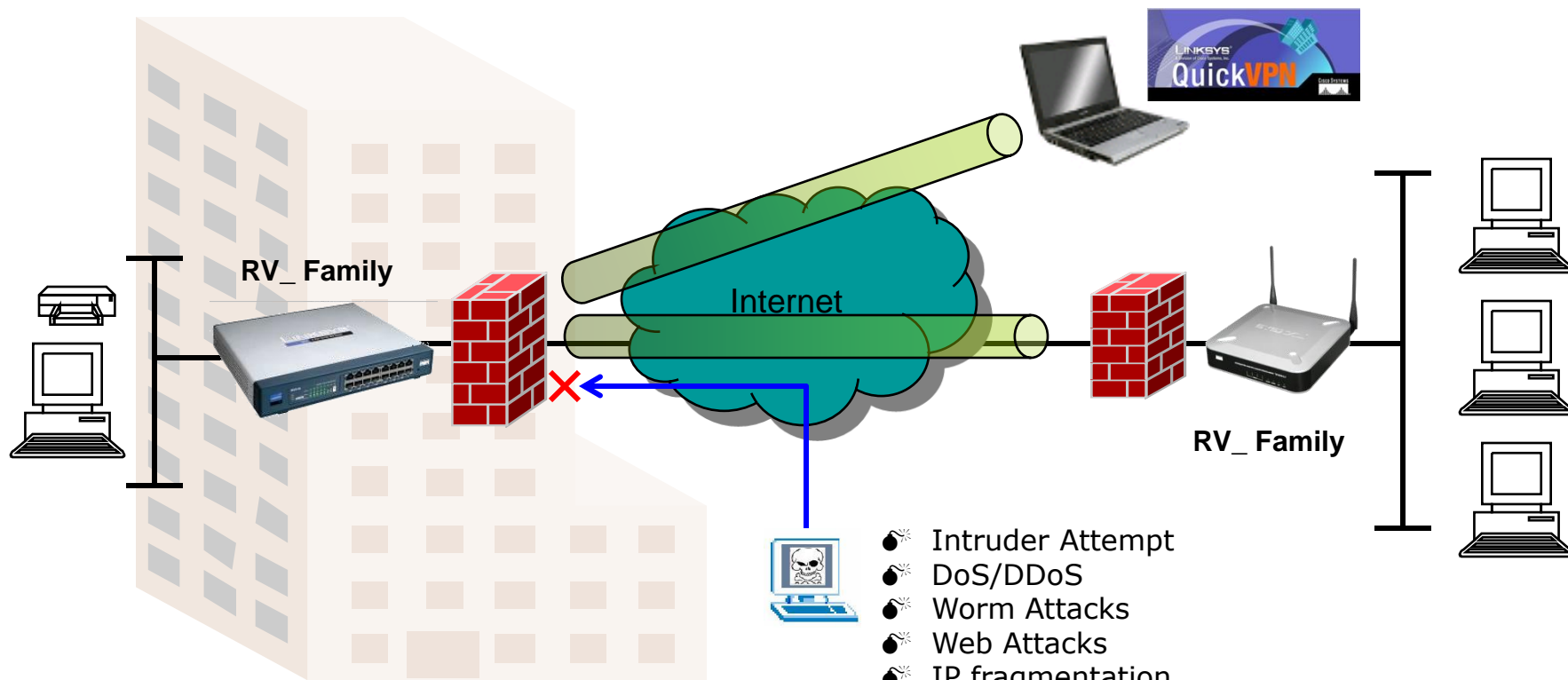
Approved Clients list	(Max. 20 IP addresses)
192.168.3.6	

Example:
IP: 10.1.1.1
IP range: 10.1.1.0-10.1.1.10
(Separate multiple entries >with semicolons)

URL Overflow Control

- Temporarily block URL requests(This is the recommended setting)
- Temporarily bypass Trend Micro URL Filtering for requested URLs

Przykład rozwiązania



- Firewall
- Intrusion Protection System (modele RV5)
- Połączenia redundantne (modele RV0xx)

- Intruder Attempt
- DoS/DDoS
- Worm Attacks
- Web Attacks
- IP fragmentation
- Trojan Horse / Back Door
- Port Scan
- Buffer Overflow
- Vulnerabilities Attacks

Punkty dostępowe

- Biznesowy zestaw funkcji, w tym funkcji bezpieczeństwa
- Możliwość zasilania przez PoE lub zasilacz zewnętrzny
- Zewnętrzny punkt dostępowy WAP200E (zasilanie tylko przez PoE) z obudową odporną na działanie warunków atmosferycznych (zgodny z NEMA IP53)
- Obsługa wielu SSID (MSSID) i funkcja mapowania SSID do sieci VLAN
- Zarządzanie: interfejs webowy, SNMP



WAP czyli bezprzewodowy punkt dostępowy

Do zastosowań zewnętrznych

802.11g MIMO



WAP200E

802.11n MIMO

Do użytku wewnętrznego



WAP200



WAP2000



WAP4410N

WAP4400N

- Obsługa silnych branżowych standardów bezpieczeństwa w tym WPA2 Enterprise
 - Zintegrowany moduł detekcji obcych punktów dostępowych (tylko WAP4410N)
- Obsługa wielu wirtualnych sieci bezprzewodowych MSSID (z wyjątkiem WAP4400N)
 - Quality of Service dla obsługi aplikacji czasu rzeczywistego w tym głosu i wideo
 - Mapowanie wirtualnych sieci bezprzewodowych do sieci VLAN (SSID to VLAN)
 - Konfiguracja oparta o interfejs webowy

WebView – Wireless VPN Router

LINKSYS
A Division of Cisco Systems, Inc.

Firmware Version: V1.1.06A

Setup | Wireless-N Gigabit Security Router with VPN | WRVS4400N

Setup | **Wireless** | Firewall | VPN | QoS | Administration | IPS | L2 Switch | Status


[Summary](#) | WAN | LAN | DMZ | MAC Address Clone | Advanced Routing | Time | IP Mode

Summary

System Information

Firmware Version:	V1.1.06A	DRAM:	64MB
CPU:	STAR 9202	FLASH:	8MB
System up time:	10 days, 04:17:26		

Port Statistics



Network Setting Status

<u>LAN IP:</u>	192.168.1.1		
<u>WAN IP:</u>	74.161.35.231	<input type="button" value="Disconnect"/>	<input type="button" value="Connect"/>
<u>Mode:</u>	Gateway		
<u>DNS1:</u>	205.152.144.23		
<u>DNS2:</u>	205.152.132.23		
<u>DDNS:</u>	Off		
<u>DMZ:</u>	Off		

Firewall Setting Status

<u>DoS(Denial of Service):</u>	On
<u>Block WAN Request:</u>	On
<u>Remote Management:</u>	Off

IPSec VPN Setting Status

<u>IPSec VPN Summary:</u>	
Tunnel(s) Used:	0
Tunnel(s) Available:	5

Log Setting Status

E-mail: **E-mail cannot be sent because you have not specified an outbound SMTP server address.**

CISCO

The System Summary screen displays the router's current status and settings. This information is read only. If you click the button with underline, it will hyperlink to related setup pages. On the right side of the screen and all other screens in the Utility will be a link to the Site Map, which has links to all of the Utility's tabs. System up time: The length of time in Days, Hours, and Minutes that the WRVS4400N is active. Firmware version: The current version number of the firmware installed on this unit.

[More...](#)

WebView – Wireless VPN Router

LINKSYS
A Division of Cisco Systems, Inc.

Firmware Version: V1.1.06A

Wireless-N Gigabit Security Router with VPN **WRVS4400N**

VPN

Setup | Wireless | Firewall | **VPN** | QoS | Administration | IPS | L2 Switch | Status

Summary | IPsec VPN | **VPN Client Accounts** | VPN Passthrough

VPN Client Accounts

Username:

Password:

Re-enter to Confirm: **Add/Save**

Allow User to Change Password: Yes No

VPN Client List Table

No.	Active	Username	Password	Edit/Remove
1	<input type="checkbox"/>			<input type="button" value="Edit"/> <input type="button" value="Remove"/>
2	<input type="checkbox"/>			<input type="button" value="Edit"/> <input type="button" value="Remove"/>
3	<input type="checkbox"/>			<input type="button" value="Edit"/> <input type="button" value="Remove"/>
4	<input type="checkbox"/>			<input type="button" value="Edit"/> <input type="button" value="Remove"/>
5	<input type="checkbox"/>			<input type="button" value="Edit"/> <input type="button" value="Remove"/>

Certificate Management

Certificate Last Generated or Imported: 2007-08-23 22:30:38

CISCO

You can allow remote users to easily establish a VPN connection to your router using the Linksys VPN Client utility to access resources on your local network.

[More...](#)

Routery / AP- dekodery produktów

Routery

- RV = Router z obsługą połączeń VPN
- RVL = Router z obsługą połączeń VPN (w tym SSL)
- RVS = Router z VPN i systemem Intrusion Prevention (IPS)
- WRV = Router Wi-Fi z obsługą połączeń VPN
- WRVS = Router Wi-Fi z VPN i systemem Intrusion Prevention (IPS)

Punkty dostępowe

- WAP = Wireless Access Point



Punkty dostępowe – akcesoria



HGA7S
Współpracuje z WAP2000



HGA9N
Współpracuje z WAP200E

**Anteny o dużym zysku ze złączami R-SMA i N-type
Umożliwiają powiększenie zasięgu działania
Twojej sieci bezprzewodowej**

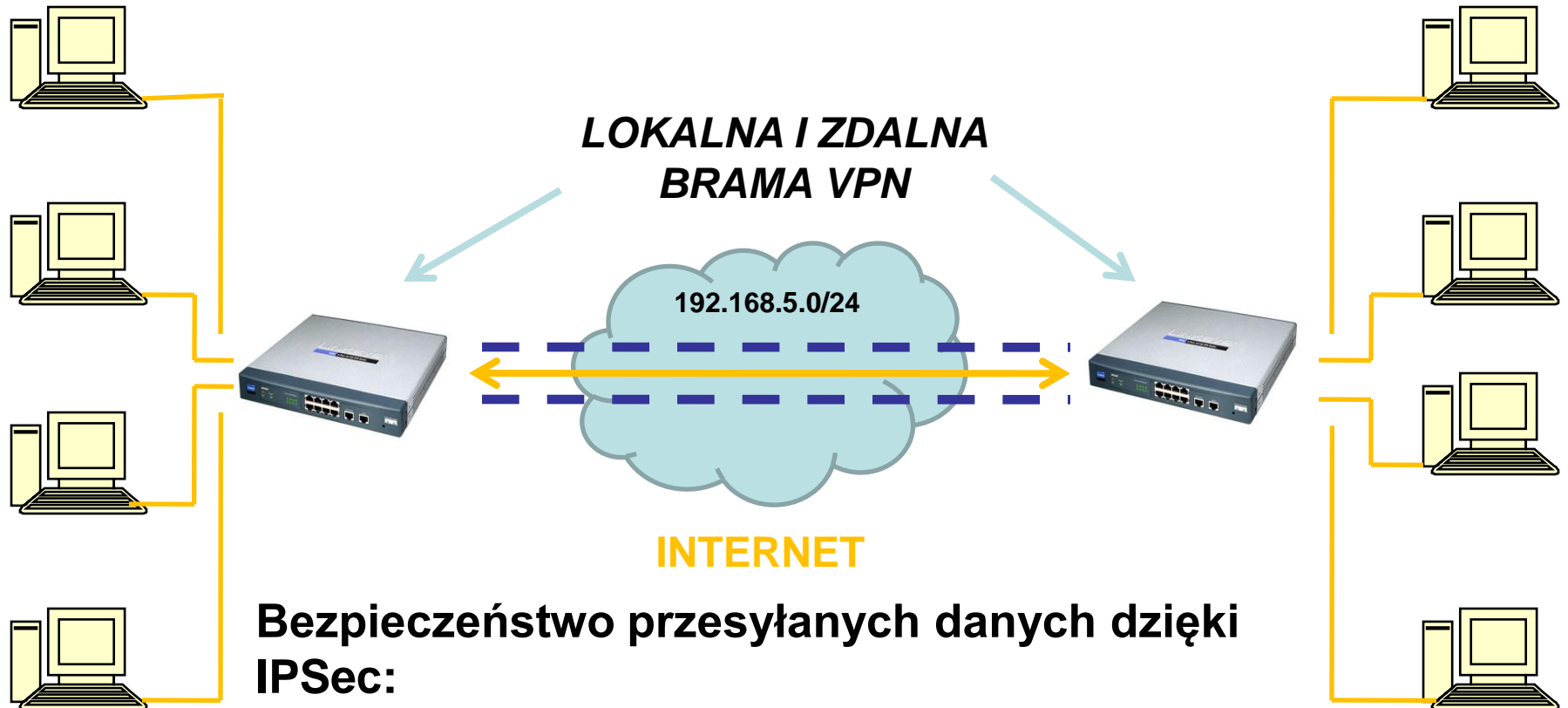
Część praktyczna

- Topologia sieci
- Konfiguracja tuneli VPN typu Gateway – Gateway na przykładzie routerów RV042
- Konfiguracja Quality of Service
- Opcja – konfiguracja tuneli Gateway – Client z wykorzystaniem oprogramowania Linksys Quick VPN Client
- Dokumentacja konfiguracji tuneli dostępna na www.fen.pl

Topologia

SIEĆ LAN 1: 192.168.20.0/24

SIEĆ LAN 2: 192.168.30.0/24



Bezpieczeństwo przesyłanych danych dzięki IPSec:

- Szyfrowanie DES/3DES/AES
- Uwierzytelnianie MD5/SHA1
- Dwufazowy proces zestawiania połączenia

