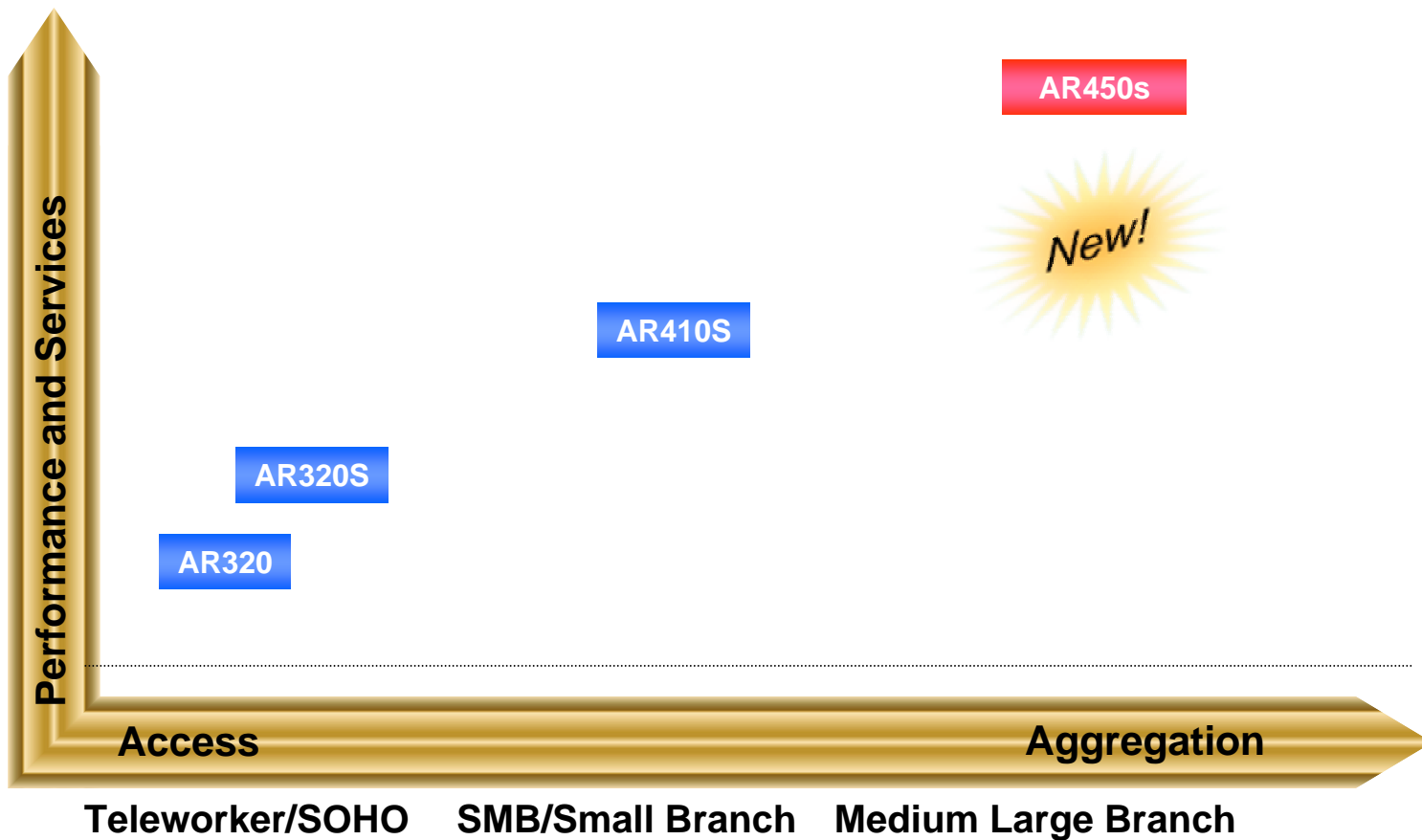


Security

Allied Telesyn Security Appliance Portfolio



AT-AR320

- Firewall ICSA-certified Stateful Inspection
- Attach Alert System
- L2TP
- PPPoE
- Protection against Denial of Service attacks
- PAP/CHAP user authentication
- RADIUS/TACAS look-up
- SMTP and HTTP Proxy
- 2 Ethernet Ports
- 2 Async Ports

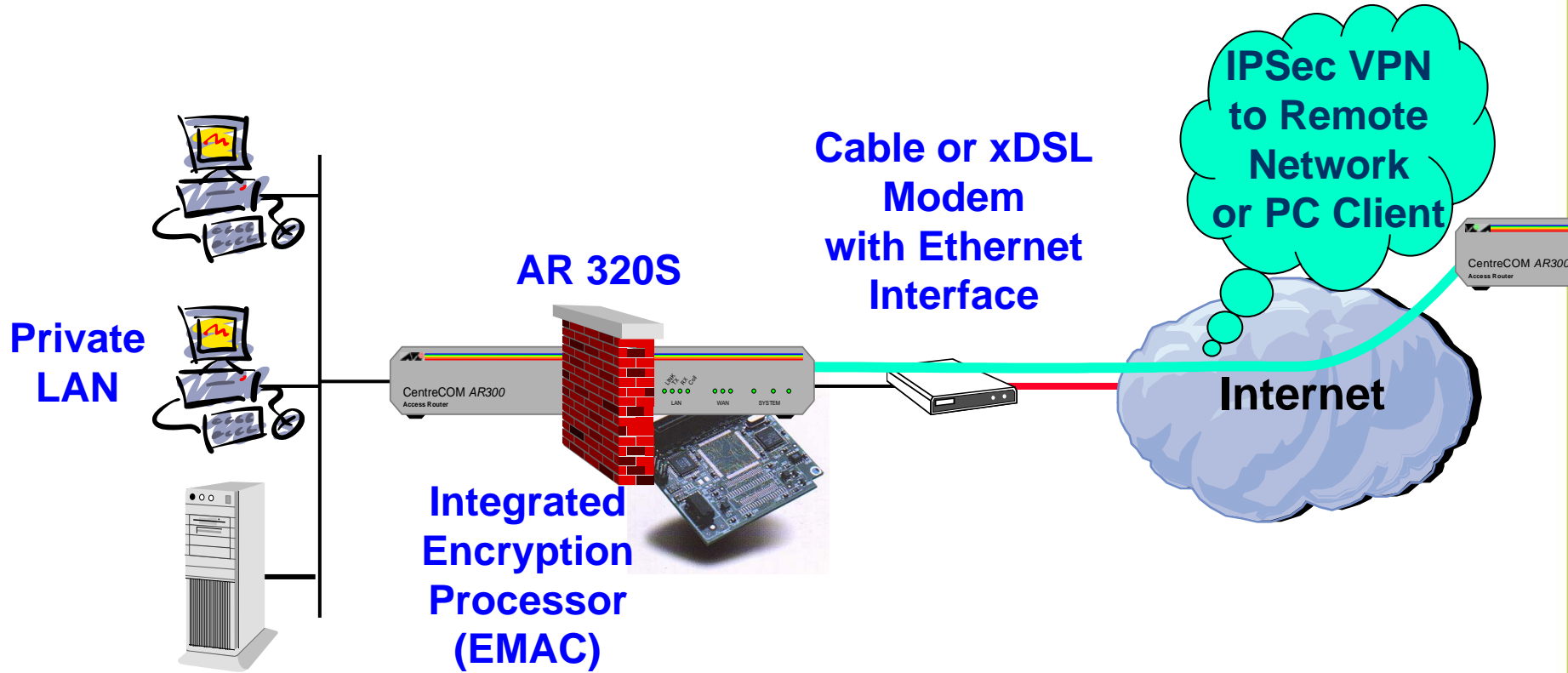
ICSA Labs Certified Firewall Product

AT-AR320S

- 60 IPSEC/ISAKMP VPN
- Hardware based DES and 3DES encryption
- Firewall ICSA-certified Stateful Inspection
- Attach Alert System
- L2TP
- PPPoE
- Protection against Denial of Service attacks
- PAP/CHAP user authentication
- RADIUS/TACAS look-up
- SMTP and HTTP Proxy
- 2 Ethernet Ports
- 2 Async Ports

ICSA Labs Certified Firewall Product

AR 320S - Adding VPN



AT-AR410S

- 256 IPSEC/ISAKMP VPN
- Hardware based DES and 3DES encryption
- Firewall Stateful Inspection
- Attach Alert System
- L2TP
- PPPoE
- Protection against Denial of Service attacks
- PAP/CHAP user authentication
- RADIUS/TACAS+ look-up
- SMTP and HTTP Proxy
- SSH SSL
- 4 Ethernet 10/100Mbps LAN Ports
- 1 Ethernet 10/100Mbps WAN Port
- 1 PIC WAN (ISDN BRI/PRI/E1, Frame Relay, X25, Leased Line)
- 1 Async Ports
-

AT-AR450S



Memory / Hardware

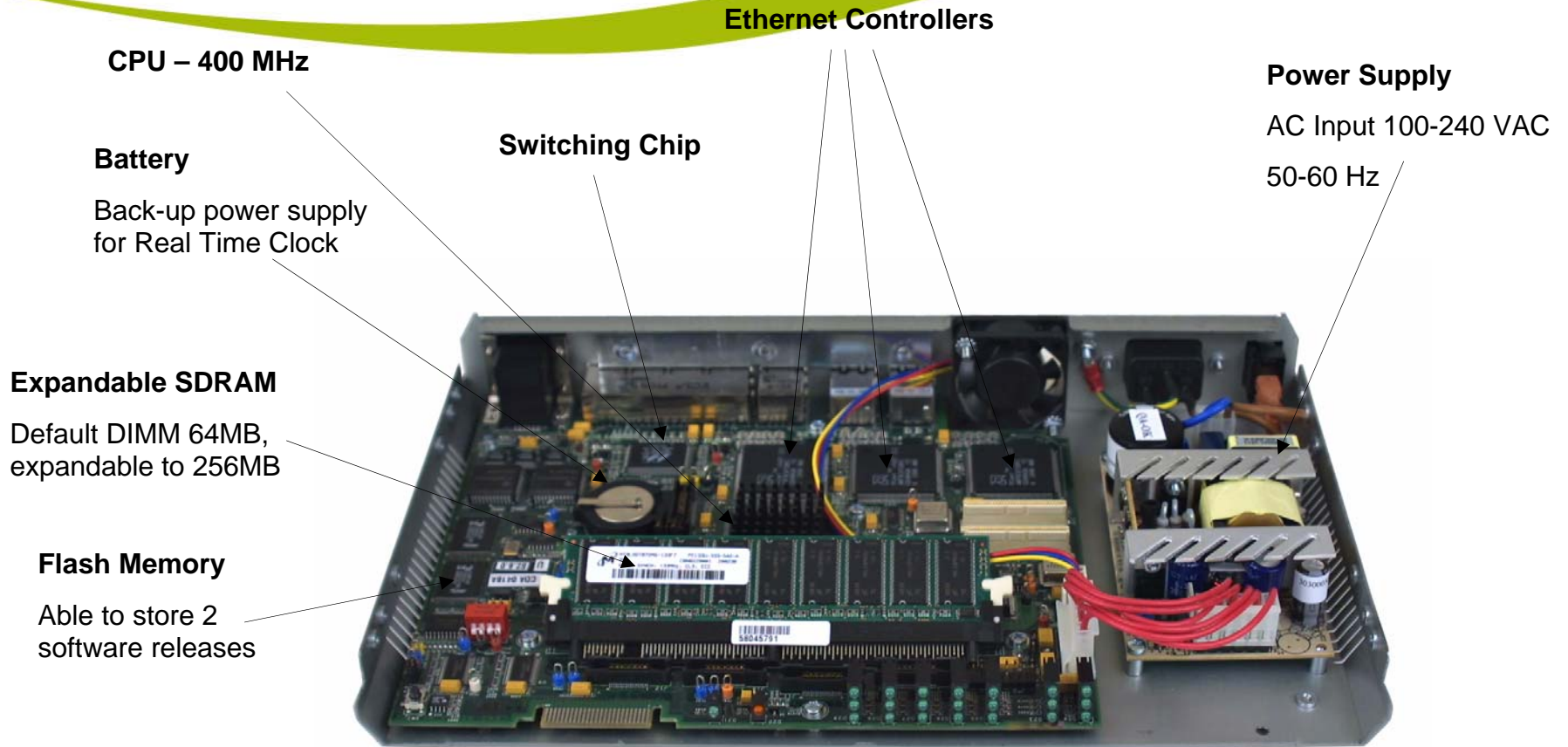
- On board security processor enabling the following advanced encryption functions:
 - Complete processing of IPSec header and trailer
 - 3DES, DES, DES-MAC, AES, SHA-1 and MD-5
 - PKI acceleration for Diffie-Hellman, RSA and DSA
 - D-H negotiation (with 1024-bit modulus, 180-bit exponent)
 - 1024-bit Sign and Verify RSA and DSA
- Core processing operating speed 400MHz
- Expandable SDRAM support – 64MB, 128MB, 256MB
- Flash Memory 16MB (default) – 32MB (Max)

AT-AR450S



- 5x 10/100 Ethernet LAN Ports
 - Auto sensing MDI/MDI-X
 - 802.1q tagged VLANs
 - Support for up to 64 VLAN Ids
- 1x 10/100 Ethernet WAN Port
- 1x 10/100 Ethernet DMZ Port
- 2x Asynchronous (RS232) ports
 - Asynchronous Serial Data Rates up to 115 kbps

AR450S Engineering



AR450S Performance

| | |
|------------------------------------|------------------------|
| Concurrent Sessions (Firewall NAT) | 18,000 |
| Firewall/NAT PPPoE throughput | 100 Mbps |
| IPSec 3DES +Firewall | 65 Mbps |
| IPSec AES +Firewall | 65 Mbps |
| # Policies | 1024 |
| LAN 10/100 Ports | 5 |
| LAN Connectivity | Fast Ethernet 10/100TX |
| WAN Port | 1 |
| DMZ Port | 1 |
| Asynchronous Port(s)* | 2 |
| Asynchronous Data Serial Rates | up to 115 kbps |

* 2x male DB9 Connectors

AR450S Protocols

Industry standard routing protocols such as

- OSPF
- BGP4
- RIP v1 & v2

Complete Multicast Protocol Implementation

- DvMRP
- PIM-SM, PIM-DM

Advanced Traffic Capabilities

- GRE
- Load Balancer
- IP Multihoming

AT-AR450S



Graphical User Interface (GUI)

The AR450S innovative Graphical User Interface allows for swift, pain free configuration and management.

Incorporated in the AR450S GUI are the following major new features:

- Easy config wizard for connection to the Internet
- PPP over Ethernet configuration and monitoring
- DHCP server configuration and monitoring
- Firewall configuration and monitoring, ability to view events, logs and device status
- Ipsec configuration

AR450S GUI Firewall Interface page



AR450S Router

Firewall Interfaces

Version 2.5.2 Serial No. 58046905

Help Save Exit

Configuration Interfaces Policy options

- Quick Start
- Configuration
 - System
 - Port
 - Layer 2
 - Internet Protocol
 - DHCP Server
 - Firewall
 - Interfaces
 - NAT
 - Traffic Rules
 - Events
- Monitoring
 - System
 - Status
 - Hardware Details
 - L2 Fwning Database
 - ARP Table
 - IP Route Table
 - PPPoE Limits
 - Log
- Management
- Diagnostics

Default configuration for a firewall with a DMZ: All traffic is allowed out the LAN interfaces to the WAN and DMZ interfaces; All traffic is allowed out the DMZ interface(s) to the WAN interfaces; All traffic coming into the LAN and DMZ interfaces is blocked.

Firewall configuration using a DMZ (Demilitarized Zone).
A DMZ is a quarantine area for servers that may become compromised. It provides additional security between a private network and an external public network. Typically, a DMZ allows specific applications and network services to be reached from the public network whilst walling off the private network.

Allied Telesyn

Copyright © 2002 Allied Telesyn International. All Rights Reserved.

Firewall Security



Allied Telesyn's state of the art ICSA-certified Stateful Inspection Firewall provides a high level of security by providing full application-layer awareness without breaking the client/server model.

- Offers per packet dynamic access control (stateful inspection) for all traffic reaching the firewall.
- Protects against a wide range of Denial of Service (DOS) attacks, including Ping of Death, Smurf attacks, port scans, fragment attacks and IP Spoofing.
- Sends automatic email alerts to initiate appropriate action.

Example - VPN Solution

