

CITADEL Series - Security and VPN Appliances

Key Features

Designed for the small business, the CITADEL Secured Traffic Shaping Router Series is a compact, feature-rich, network and security appliance. It is a great choice for cost-effectively protecting satellite and temporary offices, kiosks or replicated locations such as retail store outlets, gas stations, restaurants as well as Insurance company agents and branch offices.

CITADEL-Wizard™

CITADEL Wizard™ is an intuitive wizard providing step-by-step assistance to setup the router in a few minutes, saving time and effort during initial setup.

CITADEL-Commander™

Enables the user to configure and control the router, view the status report, upgrade firmware and perform other maintenance tasks through the CITADEL-Commander™ web interface with ease.

Rock Solid Security

CITADEL-Series Routers offer the customer a perfect security solution by full-range VPN and stateful firewall support. The intensive security mechanism repels malicious attacks from hackers, secures the precious data from eavesdropping, and protects users from any loss. All this with minimal performance impact.

Advanced Traffic-shaping Engine

CITADEL's Traffic-shaping engine helps the network manager to manipulate network traffic in a more granular manner. Network manager can adjust bandwidth consumption to adapt to real applications and fine-tune network utilization for specific components of the



network, for example: a policy can be set to limit bandwidth for P2P applications like Kazaa, eMule etc., thus saving bandwidth for business-critical applications.



Local Security and Online Monitoring by Optional USB Web

Camera

CITADEL-Series is equipped with one USB port, which gives users the option to install WEB camera for local security and online monitoring. Motion detection, along with e-mail alert, informs users of instant happenings.

Fail-Over and Load-Balancing, Increased Availability

Guarantee

To improve availability and reliability, CITADEL-Series delivers a two-tier fail-over mechanism. All CITADEL appliances support entry-level fail-over between WAN and Serial line. In addition, -200 and -200W models offer increased Internet, VPN uptime, and boosts performance by supporting two broadband links on a single CITADEL Router.

The two broadband links can be terminated at different providers and provide more bandwidth to the users. Any link failure will automatically switch traffic to another operational link with the help of the built-in fail-over mechanism. The load-balancing feature, at the same time, not only escalates the performance of the whole network, but also optimizes network utilization.

DMZ - De-Militarized Zone, Adapts more Security Options

CITADEL-Series supports two-tier DMZ (De-Militarized Zone) applications (software and hardware). All CITADEL-Series appliances support software DMZ via a hardened secure kernel. For CL-200 and CL-200W models, the additional WAN port can be implemented as hardware DMZ port. This gives the administrator a convenient option to leverage security policy and productivity, especially for remote and mobile users. With the help of DMZ setting, administrator can define different security zones on a network to host different services and servers. For example, the internal network can be reinforced with the strictest security rules, while hosts such as web server and email server can be placed in a relatively open environment on the DMZ.



Specifications

Hardware Configuration

- * 1 WAN (10/100Mbps auto-sensing Ethernet) for CL-100 and CL-100W
- * 2 WAN (10/100Mbps auto-sensing Ethernet) for CL-200 and CL-200W
- * 4 LAN (10/100Mbps auto-sensing Ethernet)
- * 1 Serial (RS232), DB9 connector
- * 1 USB

IPSec VPN

- * ESP and AH payloads
- * 168-bit 3DES encryption
- * Hashes HMAC - MD5 and SHA-1 authentication
- * IKE/ISAKMP Diffie-Hellman key exchange
- * Site-to-Site (initiate and terminate)
- * Free Dynamic DNS IPSec support

PPTP VPN

- * PPTP client and server (v2)
- * Pass-through mode
- * MPPE 40 to 128-bit RC4 encryption
- * PAP/CHAP/MS CHAPv2 authentication

Firewall & Packet Filtering:

- * Stateful firewall



- * Connection tracking & Packet inspection
- * Filters / Software DMZ
- * DoS Attack Prevention

IDS (Intrusion Detection System)

- * Anti-intrusion & logging
- * Intrusion Detection

Network Services:

- * DHCP Client, server
- * WAN Clone (MAC address clone)
- * PPPoE Client
- * NAT- Static or Dynamic
- * NAT/PAT- Port forwarding
- * NAT traversal
- * Connection sharing
- * Local and remote logging
- * DDR- Dial on Demand
- * Remote Dial-in
- * Fail-over and high availability
- * Dynamic DNS
- * 802.1d, 802.1h Bridging
- * IP aliases
- * NTP client & server
- * NetMeeting, MSN, Games, etc. pass-through
- * Static and dynamic routing



* RIP v1 & v2

WLAN-802.11b/g

- * DSSS (Direct Sequence Spread Spectrum)
- * Various data rate: 1Mbps/2Mbps/5.5Mbps/11Mbps/54Mbps
- * External Antennas x 2
- * Transmission Range: (Depends on environment)
Indoor: 130ft (40m)
Semi Open: 330ft (100m)
Outdoor: 1500ft (457m)
 - Working frequency:
 - 2.412 – 2.462GHz (North America)
 - 2.412 -- 2.484GHz (Japan)
 - 2.412 – 2.472GHz (Europe ETSI)
- * WEP & WPA
- * MAC Address Filtering

Main Server Types

- * File server (external USB disk required)
- * Print server
- * WWW server (external USB disk required)
- * FTP server (external USB disk required)
- * Email server (external USB disk required)
- * RAS (Remote Access Server)

Management

- * Easy management via any web browser
- * HTTP, Telnet



- * SNMP v1 & v2
- * Status LEDs
- * Reset Button
- * Unlimited user

Dimension & Circumstance

Dimension - 215 x 138 x 32mm (8.5"x5.4"x1.3")

Power – 110V to 240VAC, 12W

Weight - 0.5kg (1lb)

Operating temperature 0C to 40C (32F to 104F)

Storage temperature -20C to 70C (-4F to 158F)

Humidity 10 to 90%, non-condensing

CITADEL-Series Models Comparison Table

Model	CL-100	CL-100W	CL-200	CL-200W
WAN	1	1	2	2
IPSec VPN Support	√	√	√	√
WLAN AP (802.11b/g)	No	√	No	√
Fail-over & Load-Balancing	Entry-level	Entry-level	Advanced	Advanced
DMZ	Software	Software	Hardware	Hardware