



perfecting the art of network security

Features and Benefits

- *Designed for both wired and wireless networks—provides integrated security and reduced network complexity saving you network support costs.*
- *Flexible application layer (Layer 4) policy based access control—controls user access to specific applications, not just on/off (Layer 2) or network segment (Layer 3).*
- *Quality of Service (QoS)—provides more flexible management of your diverse user bandwidth requirements.*
- *Browser based authentication—no extra client software needed ensuring users ease of use, while making it easier to support a transient user community.*
- *Support for RADIUS, LDAP, Active Directory and NTLM—compatibility with these widely used authentication services means easier integration into your networks.*
- *Fully customizable authorization process—software supplied as user-customized Perl programs.*

Focused network security appliances that provide strong access control to wired and wireless networks and application layer policy based management of network resources.

Network administrators are faced with some serious security challenges when implementing wireless technology or providing public access points in places like classrooms, hospital wards, and conference rooms. When a user logs in through a wireless access point or plugs into a classroom jack, how do we really know who that user is? And once a trusted user is allowed on the network, how can you make sure they only get access to authorized network resources?



Top Layer Network's Secure Edge Controller and Secure Core Controller were specifically designed to help you plug those security holes in your wired and wireless networks and, using Top Layer's deep packet inspection capability, give you application layer control of your users' access to critical network resources.

Complete Control over Network Access

The Secure Edge Controller sits at or near the edge of the network, watching for traffic from an unauthenticated user. It blocks all this traffic before it even makes it onto the network. Only web traffic and maintenance traffic are allowed from an unauthenticated user, and all this traffic is automatically redirected to a special web server known as the Authorization Server, which prompts the user for the information necessary for authorization. This session is completely customizable for each installation, allowing total flexibility in the design of the authorization process. From something as simple as requiring that the user agree to Terms of Use through more complex schemes requiring ID's and passwords, the authorization process is entirely flexible. For those requiring access control of thousands of users like a hospital or small campus, the Secure Core Controller is the appliance to meet your needs.

Provides Fine-Grained Control and Security Policies

Once a user is authenticated, policies dictate the rights the user has on the network; thus, controlling not just the destinations that the user is allowed to connect to, but also the protocols they are permitted to use, once connected. For example, it can allow web access, FTP, and email, while disallowing streaming media. This control at the application level precludes the need to provide control with VLANs or IP subnetting.

Compatible with any User Workstation and Operating System

Because the Secure Controller uses a web-based authentication process, it is compatible with any workstation that has a web browser. The use of a web browser as the client in the authentication process ensures ease of use for the user. It also allows much faster and easier customization of the authentication process using standard off-the-shelf tools. If you have a Windows environment, the Secure Controller will integrate seamlessly into that environment with single signon support.

Integration with Existing Authentication Methods

The Secure Controller directs users into a dialog with the Authorization Server in order to authenticate them and determine the appropriate policies to apply to their network traffic. To achieve the authentication and to retrieve the user's service class, the Authorization Server interfaces to an existing authentication service using either

RADIUS, LDAP, Active Directory, or NTLM. This simplifies deployment of the Secure Controller into existing networks by eliminating the need to duplicate resources.

Resistant to Attack

Communication between the Secure Controller and the Authorization Server is both authenticated and encrypted. This provides resistance against an attack attempting to compromise the integrity of the authentication process. Unauthenticated users are allowed to send only DHCP, DNS, and ICMP traffic ensuring that until authentication takes place, those users are unable to use or abuse network resources.

Technical Specifications

Network Interfaces:

(12) 10BASE-T/100 BASE-TX (RJ-45)
(2) 1000BASE-SX (SC connectors)

Clients Supported:

Windows 98/2K/NT/XP/ME
Macintosh
Linux
Unix

Performance:

Up to 4000 users

Quality of Service (QoS):

Deny Access
Weighted Priority
Guaranteed Bandwidth
Graduated Priority
Bandwidth limiting

Policy Management:

At Layers 2, 3, and 4

Authentication Servers Supported:

RADIUS
LDAP
Active Directory
NTLM

System Management:

Web-based (GUI)
Command line interface
Telnet
Syslog reporting

Dimensions:

Height: 6.5 cm (2.55 in)
Width: 43.8 cm (17.25 in) without
rack-mount bracket
48.6 cm (19.13 in) with
rack-mount brackets
Depth: 33 cm (13 in)
Weight: 5kg (11 lbs).

Environmental:

Operating Temperature: 0° to 40° C
(32°F to 104°F)
Non-Operating Temperature: 25°C to 70°C
(-13°F to 158°F)
Relative Humidity: 5% to 95%
non-condensing.

Redundant Power Supply (optional)

Power Requirements:

AC Input Voltage: 100 to 250 VAC
auto ranging
AC Input Line Frequency: 47 to 63 Hz
AC Current Amps: 1.0
DC Output Voltage: 48 VDC +/-5%,
Watts: 48.00

International Compliance Approvals:

UL Listed
CUL
AS//NZS 3260
CE
FCC Class A
BSMI CNS 13438 Class A
VCC Class A
AS/NZS 3548 1995

About Top Layer

Founded in 1997, Top Layer Networks delivers proven network security solutions worldwide, enabling enterprises to protect against cyber threats and scale their infrastructure to meet new, ever increasing security demands. The Company's intrusion prevention products are built on a patented, ASIC-based architecture. The products are engineered to block high-volume DoS and DDoS attacks, HTTP worms, traffic anomalies, and unknown attacks; improve the effectiveness of intrusion detection systems through intelligent balancing and distribution of traffic; and enhance the availability and performance of firewalls through firewall/VPN balancing technology. Top Layer Networks is headquartered in Westboro, Massachusetts with sales and support presence in Australia, France, Germany, Japan, Korea, Malaysia, Singapore, and the United Kingdom.



Top Layer Networks, Inc. 2400 Computer Drive • Westboro, MA 01581 USA • 508.870.1300 • Fax 508.870.9797

www.TopLayer.com