

IDENTITY CENTRIC CAMPUS NETWORKS

Going beyond the UTM

UTMs are specialized *threat management* devices that protect your network from malicious traffic. Organizations today need to look beyond managing security alone. As users and uses become more sophisticated, security while important, is only part of the story. What's required is a more holistic approach to both building and managing modern campus networks.

The MSG Campus Edition consolidates your entire networking closet (or rack) into a single, intelligent, intuitive network appliance. More significantly, the MSG enables an identity centric, profile based network infrastructure that adapts network behavior and resources based on user identities.

While traditional networking devices provide most of the core functionality desired, the challenge is making them work together to easily achieve your policy objectives.

These challenges include tasks like building seamless security compliance, efficient allocation of bandwidth, network admission control and managing user activity. What's required is a more holistic approach to both building and managing modern campus networks.

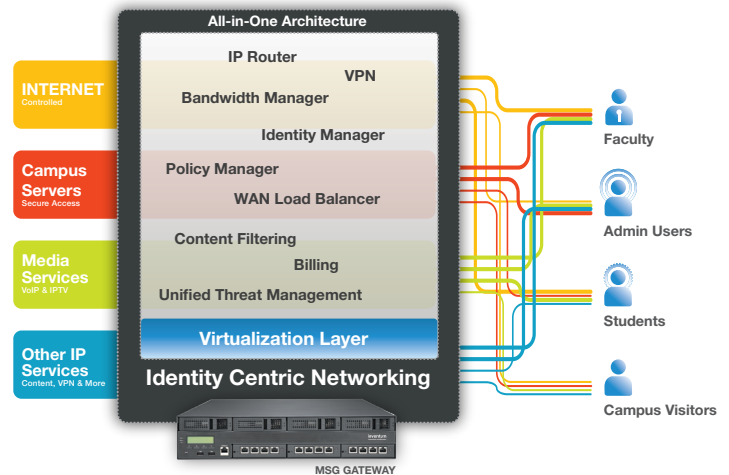
Virtualization for the Network

Server virtualization has revolutionized computing by offering on-demand, customized computing environments. The MSG brings *identity centric virtualization* to the network. Each session operates inside a personalized environment which allows unprecedented control of your network traffic. For example, each session can have personalized routing, security filters & QoS.

Virtualization profiles encapsulate the entire configuration information required for all MSG sub-systems. Using a browser GUI, administrators manage these profiles while the underlying networking blocks are automatically configured and validated by the MSG to avoid conflicts and mistakes in your network.

Virtual Engines

- **IP Router** - Standards based static and dynamic routing. Identity based session routing.
- **Unified Threat Management (UTM)** - Firewall, IP filtering, gateway anti-virus, anti-spam, personalized content filtering & IPS with on-board hardware acceleration engine to boost performance.
- **Policy & Identity Management Engine** - Design, store & enable user policies directly on the MSG. Support real-time query of external policy servers (RADIUS, LDAP, Windows ADS) on a per user basis. All policies are automatically applied as and when the user is detected or authenticated on the network.
- **Bandwidth Management Engine** - Enable dynamic QoS



Consolidation & virtualization for your network infrastructure including IP Router, UTM, Bandwidth Manager & more.

capabilities based on nature of traffic & user identity. Personalize network experience while catering for latency sensitive applications, peak & off-peak traffic handling. For example, student and faculty profiles can have different QoS and time-of-day policies.

- **VPN Engine** - IPSec, L2TP and PPTP supported. Build secure site-to-site networks with road warrior (dial-in) support using standard VPN dialers.
- **WAN Link Load Balancer** - Manages multiple ISP uplinks. Split, policy route or use as active-passive configuration to optimize your WAN bandwidth providers.
- **Session Metering & Billing Engine** - Accumulate detailed metrics and usage data for each session. Define per user quotas for network time and download limits. Isolate bandwidth abusers and optimize bandwidth distribution while discouraging misuse (P2P, Torrents). Optional billing module is perfect for reselling bandwidth to student residences, conference guests and campus visitors.
- **Analytics Engine** - User centric on device reporting and analysis including session metrics, URL logs, security logs, trends, alerts and alarms.
- **Lawful Tracking** - protect network from unlawful use particularly to comply with government regulations in specific countries and industries.

Multiple Modular Appliances



MSG-3000 Series

Feature	Description
Identity Aware Platform	<ul style="list-style-type: none"> Virtual networking per user with unprecedented session personalization. Single sign-on for all network resources.
Full Stateful Firewall	<ul style="list-style-type: none"> Complete network security. Application level filtering (Skype™, P2P) Virtual firewall table per subscriber. Out-of-the-box peace of mind.
Anti-Virus, Anti-Spam & Anti-Malware	<ul style="list-style-type: none"> Protect e-mail & web traffic without re-configuration at subscriber/user PC. Identify problems easily. Alerts administrator to potential threats. Automatic update of threat databases.
Personalized Content Filtering	<ul style="list-style-type: none"> Identity centric filters. Block unwanted content & sites. Pre-determine rouge & friendly networks. Conserve bandwidth.
Application Filtering & Deep Packet Inspection* (DPI)	<ul style="list-style-type: none"> Automatically identify network trends Control applications including P2P, VoIP, IM and more
Intrusion Prevention System (IPS)	<ul style="list-style-type: none"> Secure your network from known and future attacks. Protection works on both internal and external network threats.
Bandwidth Management	<ul style="list-style-type: none"> Optimally utilize bandwidth across your network. Avoid bottlenecks. Prioritize users and applications. Restrict users from over-use or limit network usage by schedule.
Virtual Private Network (VPN)	<ul style="list-style-type: none"> Connect multiple campuses or remote users securely. Use industry standard protocols. Optional customizable cryptography hardware allows higher level of security for strategic networks.
Administration	<ul style="list-style-type: none"> Easy administration using browser & secure shell (SSH) Delegate administrative tasks using role based administrative access. Alerts & updates from network
Analytics	<ul style="list-style-type: none"> On appliance, browser based reporting. SNMP & SOAP/XML support Browser for textual & graphical reports

* On select models only, upcoming release

SOLVING PROBLEMS

Can the MSG replace a UTM for security?

The MSG provides functionality that is a super-set of what a traditional UTM provides. Each user profile has a *security sub-profile* which allows administrators to configure UTM style security & protection.

Similar to a UTM, MSG supports bridge and routed modes for easy adoption. Popular networking service daemons - DHCP, DNS, NTP & NAT are provided. IPSec VPN capability allows secure site-to-site and dial-in access. Gateway level anti-malware, IPS and threat protection is standard.

What is Identity Centric Networking?

Unlike ordinary routers, switches and UTM systems, the MSG handles traffic with the context of who the traffic belongs to. To identify the owner of the traffic and hence establish the identity, the MSG uses multiple techniques. These include analyzing packets as well as forcing users to authenticate before permitting network sessions. Authentication can be for humans or even network devices using a variety of well established systems - 802.1x, web page login, Windows ADS, LDAP & RADIUS. Once identity is established, the MSG creates a personalized, virtual network for each user. Inventum refers to this as *Identity Centric Networking*.

Can I use the MSG for securing campus Wi-Fi?

MSG appliances can completely replace the function of wireless access controllers to lock-down campus access points. Simply add any WiFi access points on your network and route them to the MSG. With support for 802.1x (WPA/WPA2) and one-time visitor passwords, the MSG can authenticate users and visitors provisioning personalized sessions for each. If using multiple SSID or virtual AP, MSG can securely segregate traffic to pre-determined VLAN based on user identity. What's more, the personalized security profile associated with each user, automatically secures network access and applies content filters. The MSG can also record session history (private and public IP, URL visited) to comply with IT policy and audits.

Is bandwidth control possible with the MSG?

MSG enables per user, time-of-day and protocol based bandwidth management. Each user profile can contain a bandwidth policy which defines committed and burstable information rates. Policies can be scheduled based on time-of-day and day-of-week. Additional features include Diffserv support and multi-tiered WAN policies.

March **09**
www.inventum.cc
sales@inventum.cc

AMERICAS

Inventum International Ltd.
Suite 600 Millennium Center
15455 Dallas Parkway
Addison, Texas 75001 USA
Tel. +1 (214) 233-0659

ASIA & EMEA

Inventum Technologies (P) Ltd.
B-5, Sector 6,
Noida UP, 201301
India
Tel. +91 (120) 427 4900

©2008-2009 Inventum International Limited. All rights reserved. Inventum is a registered trademarks of Inventum Technologies Private Limited in various countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Although Inventum has attempted to provide accurate information in these documents, Inventum assumes no legal responsibility for the accuracy or completeness of the information. Please note that no Inventum statements herein constitute or contain any guarantee, warranty or legally binding representation. All materials contained in this publication are subject to change without notice, and Inventum reserves the right to change, modify, transfer, or otherwise revise this publication without notice.