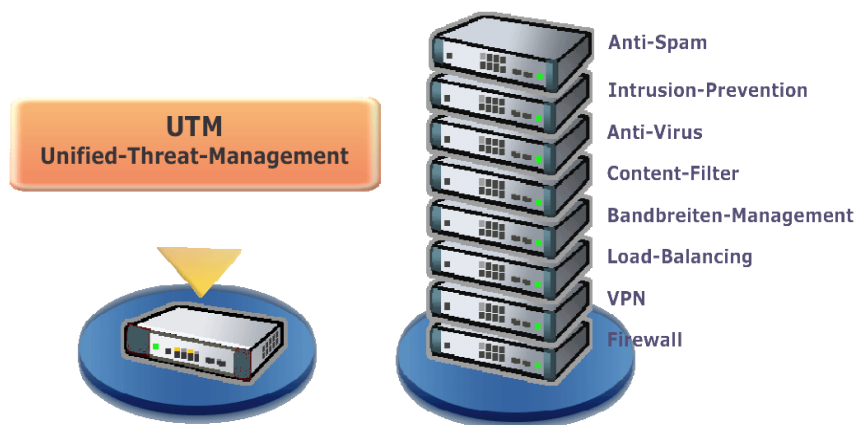


WHITE PAPER

UTM (Unified Threat Management)

Bulwark System SecuraNET is a complete, integrated UTM product. The SecuraNET UTM is a security appliance which is placed at the point where the Internet connects to your organization's network – the perimeter. It protects and secures your network eliminating the Internet perils – even from inbound and outbound traffic containing viruses and other malicious content.

SecuraNET UTM Perimeter-based protection: This security appliance is active at the Internet's point of entry to your organization - the UTM, scanning all packets and transmissions within the network and internet.



Who needs a UTM?

Anyone who is responsible for a private network that is connected to a public network needs firewall protection. Many Internet users believe that anonymity will protect them. They feel that no malicious intruder would be motivated to break into their computer. Internet users who have been victims of malicious attacks and who have lost entire days of work, perhaps having to reinstall their operating system, know that this is not true. Irresponsible pranksters can use automated tools to scan random IP addresses and attack whenever the opportunity presents itself.

THE WAY WE SERVE THIS PURPOSE

The **SecuraNET UTM** examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.

Benefits of SecuraNET UTM

UTM protects private local area networks from hostile intrusion from the Internet. Consequently, many LANs are now connected to the Internet where Internet connectivity would otherwise have been too great a risk.

Firewalls allow network administrators to offer access to specific types of Internet services to selected LAN users. This selectivity is an essential part of any information management program, and involves not only protecting private information assets, but also knowing who has access to what. Privileges can be granted according to job description and need rather than on an all-or-nothing basis.

Is a firewall sufficient to secure my network or do I need anything else?

The firewall is integral module of SecuraNET UTM. Security involves data integrity (has it been modified?), service or application integrity (is the service available, and is it performing to spec?), data confidentiality (has anyone seen it?) and authentication (are they really who they say they are?). Firewalls only address the issues of data integrity, confidentiality and authentication of data that is behind the firewall. Any data that transits outside the firewall is subject to factors out of the control of the firewall. It is therefore necessary for an organization to have a well planned and strictly implemented security program that includes but is not limited to firewall protection.

THE WAY WE SERVE THIS PURPOSE

Impenetrable Firewall: Features like Advanced stateful packet filtering and Port forwarding make the firewall highly reliable.

Content Filter: Features like expression based filtering and Filter bypass for specific IP gives product the required flexibility to cover all the range of users.

Resource Access Restriction: Blocking various Network resources like IP and ports depending upon the policies assigned.

Web Access Restriction: Blocking various objectionable web resources like websites, URL, extensions, etc.

Intrusion Detection: Detecting intrusion in various ways like port sniffing, hacking, spoofing, etc.

Intrusion Prevention: Preventing further attacks like DOS-DDOS by blocking the ports, considered to be the source of attack

Virtual private Network: 128 bit IPSec VPN and multiple concurrent VPN connections render data transfer high security and flexibility.

Gateway Load Balancing and Failover support: Traffic Management, least followed path optimization and automatic failover provide an effective utilization of network resources that effects the network access speed.

Gateway Antivirus: The antivirus provides the appliance power to scan, assess, detect, discard or quarantine any malicious HTTP, FTP, POP3, SMTP packets that intend to corrupt the network.

Internet Access Management: Time based and IP based internet access restrictions provides better control over the Network resource management.

Bandwidth Management: Bandwidth allocation and restriction based on users, applications and services also provides better control over the Network resource management.

User Management: User Management mainly follows the hierarchy, **policy to group to user** i.e. initially the policies are decided upon, after which the groups are categorized on the basis of policies and after which the users are created, which are also categorized into authenticated and non-authenticated types.

Report: Processing logs and giving a user friendly interface of various logs in form of reports.