

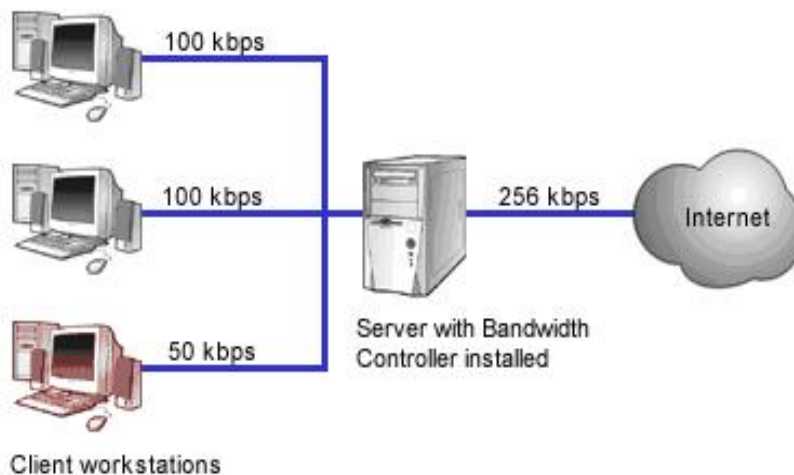
White Paper on Bandwidth Management

SecuraNET UTM offers policy-based bandwidth management based on business priorities.

SecuraNET user-based bandwidth management prevents bandwidth abuse and resultant pipeline choking through bandwidth scheduling and providing committed, burstable bandwidth, protecting enterprises from Internet productivity threats.

It allows enterprises to take control of non-business related Internet activity which often affects critical business-related usage through its unified threat management. Business policies are created and linked to network management and usage reality, ensuring success of the policy.

Through SecuraNET UTM, enterprises gain higher user and enterprise productivity through optimum use of infrastructure and smooth process of mission-critical applications.



Supporting Mission Critical Applications

SecuraNET UTM enables enterprises to maximize performance of business-critical applications by allocating bandwidth based on all TCP & UDP Ports.

Enterprises can assign committed bandwidth to bandwidth-sensitive applications like VoIP, ensuring that they do not suffer at the hands of delay insensitive applications like mail and non-business surfing.

Committed and Burstable Bandwidth

Administrators can create policies for committed and burstable bandwidth and establish priorities based on users, groups and applications with precise bandwidth allocation based on usage. This prevents non-critical applications from degrading network performance. Unutilized bandwidth is automatically allocated to user groups. Policies are finetuned for continually improved network performance despite changing requirements and usage.

Virtual Private Network: Secure Connectivity

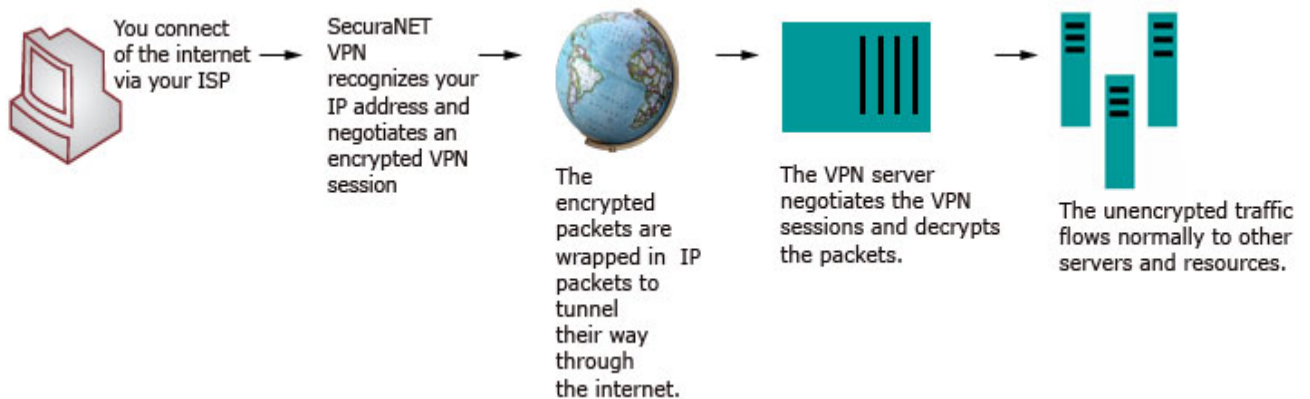
SecuraNET UTM IPSec VPN offers secure access to corporate resources for remote offices and mobile business users.

SecuraNET VPN gateway offers secure, encrypted tunnels, extending the corporate network anywhere in the world. With unmatched firewall-VPN performance and easily manageable access to corporate resources, it is ideally suited for the branch office and road warrior need for secure remote access to enterprises.

Offering high performance with low bandwidth requirements, SecuaNET VPN is a highly cost-effective solution to enterprises in the emerging mobile world.

SecuraNET VPN is interoperable and compatible with most of the VPN gateways following IPSec standards available in the market.

For road warrior connectivity, Bulwark also provides IPSec VPN Client compatible with most of the IPSec VPN gateways.



Remote Access

With advanced encryption algorithms and authentication methods, SecuraNET enables secure access to corporate resources for road warriors, telecommuters and branch offices, providing secure IPSec, L2TP, VPN for Site-to-Site and Host-to-Site connectivity.

SecuraNET VPN prevents eavesdropping and data tampering, protecting information confidentiality. In addition to verifying host and end-point integrity, SecuraNET VPN protects data integrity, ensuring that no modifications were made to the data while in transit.

Tunneling

SecurNET UTM VPN works in transport and tunneling mode, securing IP packets from the originating source to the destination as well as wrapping an existing IP packet inside another

defined in the IPSec format. With this flexibility, enterprises can have secure connectivity through different Internet service providers and network types.

This UTM supports Preshared Key based user authentication. Its NAT traversal allows IPSec connection through a NAT device.

Firewall Integration

Fully integrated with Bulwark's Firewall, the VPN functions alongside NAT and provides secure end-to-end network connectivity.

Designed to reduce the complexity of standalone solutions and enhance security, SecuraNET UTM IPSec VPN is part of Bulwark's strategic threat management solution, offering easy configuration and installation, ease of use and cost-effectiveness.