



Secure your personal computer and home network against Trojans, worms, and other attacks and securely connect to your home network from anywhere.

The popularity of always-on Internet connections and weak remote access tools means a hacker has many machines to target that may not be adequately protected. In addition to always-on connections, a computer may be compromised by a user downloading malicious software or visiting hostile web sites.

The number of compromised machines on the Internet is growing rapidly because the majority of home and small business computers do not have adequate firewalls and methods to detect and prevent intrusions. In most cases, the user may not even know that their machine is compromised.

Once a machine has been compromised, information gathered from that machine may be used for exploiting financial gains, or the computer can be used to launch further attacks. Either scenario is a disaster for the user whose machine has been compromised.

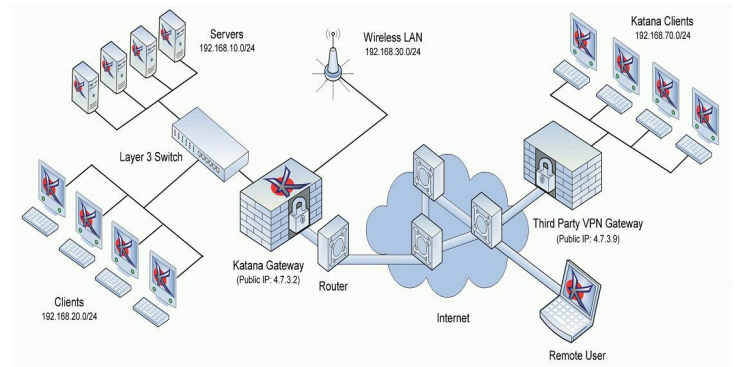
It is extremely important that all personal computers be protected by a personal firewall and any remote access be done via secure VPN.

Integrated Security Solution

Trlokum offers industry-leading solutions for end point security that are scalable and end-to-end secure.

Katana is a comprehensive enterprise-class security solution, now made available for personal and small or medium business (SMB) users. It incorporates a perimeter/desktop firewall, VPN client/gateway, wireless security, and intrusion detection and prevention solution.

End-point and Network Security



Client

To solve the end-point security problem, the Katana client incorporates three security functions:

- ✓ Firewall for the client
- ✓ IDS and IPS for the client
- ✓ VPN client

By integrating these critical security components, the overall footprint and complexity of the system are reduced while the performance, management, and security are improved.

The Katana client firewall controls the nature of network traffic entering and leaving the end point and ensures that all unauthorized traffic is blocked. To improve the firewall security, the intrusion detection system (IDS) and intrusion prevention system (IPS) control which applications can access the network and the type of traffic they can generate. With full control over the network traffic flow and the applications, any Trojans and worms that manage to defeat the perimeter defenses can be easily contained and prevented from spreading to the rest of the enterprise network. In the absence of such a solution, the network will remain very vulnerable.

To improve security and protect clients from attacks, Katana client automatically detects and





prompts the user to provide a trust level for the subnet to which the client is connected. The default is not to trust the subnet so that any attempts by other nodes on that network to connect to client will be rejected.

The VPN client component of Katana provides secure connectivity to the enterprise or home network. The configuration of VPN tunnels is simple, and the client interoperates with most third-party VPN gateways, thereby making it a great choice for those seeking end-point security and remote connectivity.

Server

The Katana server provides a high-end perimeter VPN gateway and firewall for use by SMB and home users. Most products available for SMB and personal use are extremely limited and do not function well, especially for remote access.

Katana gateway can assume the role of the perimeter firewall and VPN gateway. It can handle over 300K simultaneous network connections while maintaining 50Mb/s of sustained, 3DES-encrypted throughput using off-the-shelf hardware and will meet the needs of most SMB and home networks.

A unique feature of Katana is that it does not require static IP addresses for VPN gateways. All VPN gateways in the network can have dynamic IP address and the Katana VPN will still function. Support for NAT-traversal in Katana gateways ensures that remote nodes and gateways behind NATs will be able to establish VPN connections with Katana gateways.

Katana gateways also interoperate with most third-party VPN gateways. As the user's needs grow, the Katana client and gateway can be easily upgraded to OmniVPN.

Trlok, Inc.

Tel: 1 626 357 3706

Email: katana@trlok.com

