



**Secure your enterprise networks against internal and external threats using scalable, end-to-end secure solutions.**

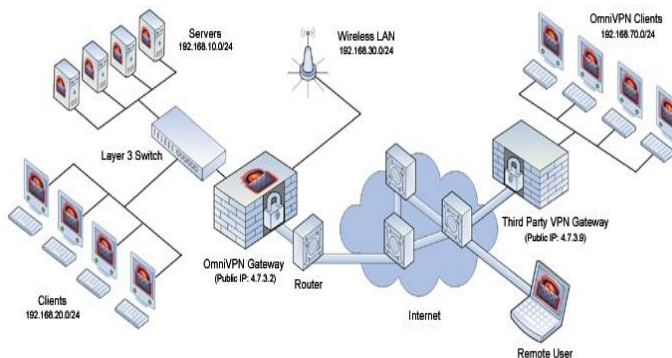
The threats against enterprise networks today are greater than ever, and the prime targets are now the vulnerable end points rather than the fortified perimeter devices. The end points in a network can be easily compromised by a user visiting a hostile web site or downloading free software that contains malicious code or by an infected host joining the local network and spreading malicious content to other hosts on that network. Improving the end point security, the weakest point of most enterprise networks, is a key ingredient of any satisfactory enterprise security solution.

Trlokum provides an integrated approach to network security and connectivity and addresses both internal and external security threats. This approach yields better security, improved performance, and reduced total cost of ownership.

## Scalable, Integrated Security

Trlokum offers industry-leading solutions for end point security that are scalable and end-to-end secure. OmniVPN is a comprehensive security solution for enterprise networks that incorporates perimeter/desktop firewall, VPN client/gateway, wireless security, and intrusion detection and prevention, all managed by a hierarchical management system that provides scalability and redundancy.

## End-point and Perimeter Security



### Client

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

- ✓ Firewall for the client
- ✓ Intrusion detection and prevention
- ✓ 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 OmniVPN client can act as a stand-alone client where the security policies are locally managed, or it can be centrally managed.

The OmniVPN client firewall controls the nature of network traffic entering and leaving the end point and ensures that 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.





When the OmniVPN client is centrally managed, it will receive security policies from the policy servers. The security policy at the server will govern whether or not the client may modify any policies locally. Software upgrades are also pushed to the client from the policy servers, thereby allowing the entire network to be upgraded remotely. In a large network, this simplifies the task of upgrading to a newer version.

The VPN client component of OmniVPN provides secure connectivity to the enterprise network. The configuration and policies for remote access can be managed centrally. Even the little configuration necessary at the client can be done remotely from the policy servers. OmniVPN clients also interoperate with most third-party VPN gateways. This makes OmniVPN a great choice for those seeking end-point security and remote connectivity.

## Server

The OmniVPN server solves the most complex problem in enterprise security, i.e., managing security policies for a large number of end points. Using OmniVPN, the VPN, firewall, and IDS/IPS policies implemented at the perimeter and at the end points can be managed centrally. The VPN and firewall policies are managed based on subnets and IDS/IPS policies are managed based on groups and roles. A hierarchical, push-based management system with server node clustering ensures that policies are updated at all points in the network with minimum delay.

To improve security and compliance with corporate security policies, the OmniVPN architecture requires that the ability to change policies for the network be explicitly granted to nodes. The only nodes with complete control over the security policies are the Top Policy Servers. Without the ability to modify local security policies, the chances of an end point permitting a Trojan are greatly reduced.

If necessary, the OmniVPN policy server can assume the role of the enterprise perimeter firewall and VPN gateway. The perimeter firewall/VPN will meet the needs of most enterprise networks with its ability to process over 300K simultaneous network connections while maintaining 50Mb/s of sustained, 3DES-encrypted throughput using off-the-shelf hardware. Several OmniVPN gateways can be clustered together to improve throughput and availability. When a particular gateway is overloaded or becomes unavailable, the local clients automatically route the traffic through other nodes in the gateway cluster. The result is high availability without the need for expensive load balancing switches or idle, hot standby machines.

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

OmniVPN gateways also interoperate with most third-party VPN gateways, and a service provider version of OmniVPN can manage multiple VPNs from the same policy server. The service provider version scales to several million nodes using hierarchical management and policy server clustering.

Trlok, Inc.

Tel: 1 626 357 3706

Email: [omnivpn@trlok.com](mailto:omnivpn@trlok.com)