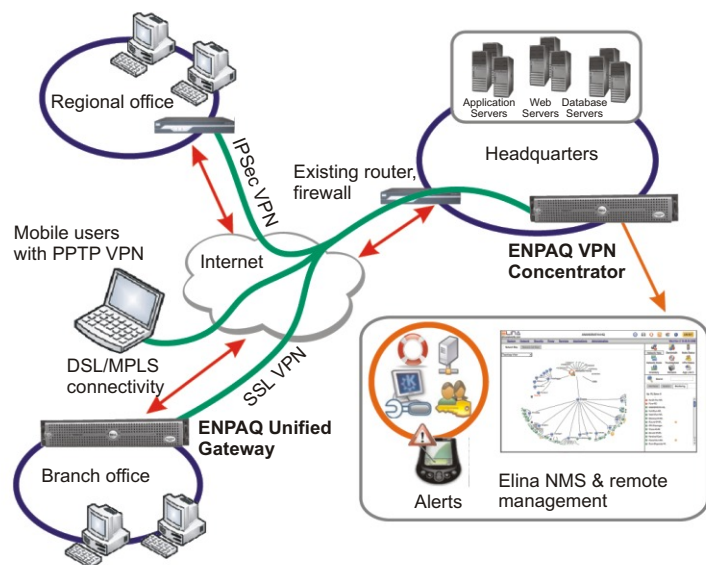


ENPAQ VPN Concentrator

Create reliable, high performance, scalable VPN connections across geographies, ISPs, and diverse network devices.

Building a Virtual Private Network over broadband is the most secure, reliable, and cost-effective way for a company to transact business across a geographically distributed area. The ENPAQ VPN Concentrator is a powerful and flexible remote access solution for Enterprises. Users can remotely access network services such as ERP, CRM or Intranet from anywhere in the world. Branches can securely connect via site-to-site VPN with ENPAQ VPN Concentrator, giving seamless, secure connectivity to business applications such as Oracle, Tally, SAP, and others. In addition the ENPAQ VPN Concentrator can be configured as a VPN firewall, router, and proxy segregating VPN and non-VPN traffic ensuring perfect security. The multiple VPN technologies, clustering and failover, VPN tunnel, user management, detailed usage reports of ENPAQ VPN Concentrator helps in providing secure, authenticated remote branch and nomadic access to servers located in the HQ or datacenter.



Flexibility

The ENPAQ offers a choice of three independent VPN technologies which can be enabled simultaneously, giving you flexibility to provide the best possible connection type to each remote user or location. For mobile users PPTP VPN is ideal with built-in PPTP client for laptops. For highest security, reliability, ease of use and fine-grained control Elina recommends the use of SSL VPN. Whereas for interoperability with heterogeneous external network devices IPsec may be used (ENPAQ conforms to IPsec/IKE RFCs and is compatible with Microsoft, Cisco, Nortel, Checkpoint, Netscreen and many other vendors).

100% Uptime

With increasing number of mobile users and remote sites accessing the essential application servers located in the head quarter DMZ, the VPN performance and availability becomes critical. Elina's VPN solution allows you to setup a clustered, multi-homed environment for high reliability with multi-ISP load-balancing and failover, ensuring 100% VPN uptime for all the users. Our customers are currently using ENPAQ VPN link as a secondary backup to an existing private leased-line, VSAT, or MPLS. The advanced link failure detection and routing mechanism of ENPAQ makes it a smooth transition for all critical branch transactions where downtime needs to be close to zero. For hardware failover and load balancing, multiple servers can be configured and the clients can automatically connect to the available servers. High availability with VRRP is supported for additional protection against hardware failures.

Scalability

Both large and small enterprises use site-to-site VPNs (hub and spoke) to communicate to their business systems. As sharing of information grows, the number of VPNs will also grow. Especially in the area where site-to-site VPNs are created for the inter-office encrypted VoIP calls and data sharing between various office locations. Using an SSL VPN to carry VoIP over TCP actually improves voice quality, according to testing done by Network World. VPNs can also provide security for VoIP calls running over Wi-Fi networks, blocking eavesdropping. Some of Elina's customers who are using SSL VPN have hundreds of concurrent users, load-balanced over multiple VPN Concentrators. These customers are very happy with the excellent scalability options provided by ENPAQ.

Security

The ENPAQ ensures secure data transfer with various certificate options. Perfect Forward Secrecy allows encryption keys to change every hour and prevent ciphering option. Client keys can be locked to source IP address and be password protected. The AntiVirus/AntiSpam, content filtering, Stateful Packet Inspection and Intrusion Detection of ENPAQ can enforce added security needed by customers. NAT traversal lets users connect from all common ISPs.

SLA Monitoring

The constant monitoring of VPN usage and prioritizing of the traffic helps the customer make most usage of the link. Customers can even reserve bandwidth for each VPN client.

Reports

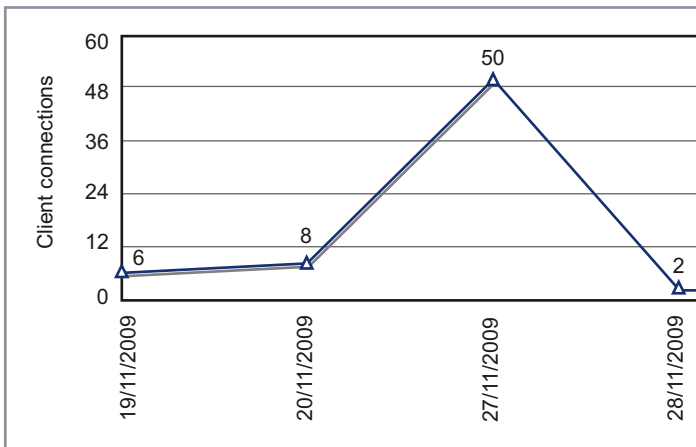
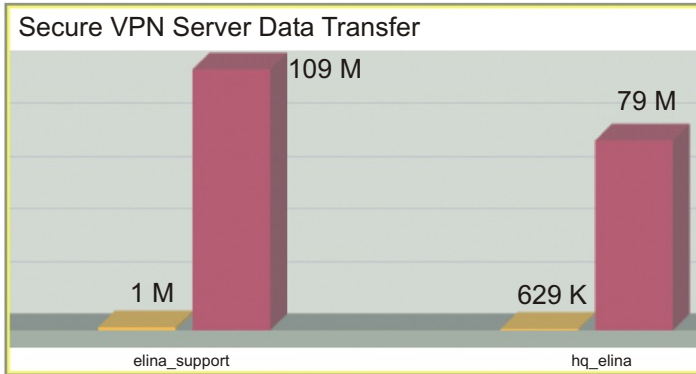
Detailed VPN server usage and top client connectivity reports are available in graphical or PDF report format.

"Elina's WAN auto-failover and VPN gave us 100% network uptime in our stores, keeping our ERP synced and improving productivity."

- Mr. Alagappan, Head IT, Spencer's Retail

- **Flexibility** – multiple VPN servers (SSL, IPSEC & PPTP VPN)
- **Reliability** – 100% network uptime with multi-ISP failover (SSL VPN)
- **Scalability** – hundreds of concurrent users load balanced over multi-ISP WAN links (SSL VPN)
- **Security** – Anti-Virus, Spam Filter, IDS/IPS & PFS
- **Manageability** – monitoring SLA of VPN links & WAN links (bandwidth, uptime)

ENPAQ VPN Concentrator



System performance

Concurrent sessions	30,00,000
New sessions per second	65,000
Firewall performance (IMIX)	Wire speed
Number of users	Unlimited
Number of firewall policies	Unlimited
Encryption, AES 256+SHA-1	40 Mbps
Encryption, 3DES+SHA-1	40 Mbps

Recommended hardware (up to 100 tunnels)*

Processor	AMD/Intel dual core processor
Memory	2GB
Disk	80 GB
Network interfaces	1 (minimum), 2(recommended)
Peripherals	No (mouse, keyboard, monitor)
Bundled OS from vendor	NO OS required ENPAQ has its built-in Linux

*Hardware sizing depends on number of users, WAN bandwidth and add-ons enabled.

Managing the ENPAQ VPN Concentrator

The best part about the ENPAQ VPN Concentrator is that your network administrator does not need dozens of certifications to get it up and keep it running! A comprehensive and easy to use Web GUI lets you create servers, create users, add routes, and add restrictions very easily.

The ENPAQ VPN Concentrator ensures smooth operation by managing the network operations centrally from a single web interface. No additional management or security tools are required to be installed, making the network configuration simpler. The easy rollout option with customer-specific default configurations are hard to match with from devices available from other vendors

Features at a glance

- Multiple VPN Servers supporting PPTP, IPSec and SSL VPN
- Multi-ISP Load Balance and Failover support via SSL VPN
- Perfect Forward Secrecy allows encryption keys to change every hour
- NAT traversal lets users connect from all common ISPs
- Site-Site and nomadic VPN clients
- Client keys can be locked to source IP address, be password protected
- Conforms to IPsec and IKE RFCs. Compatible with products from Microsoft, Cisco, Nortel, Netscreen, Checkpoint, and other vendors
- AntiVirus/AntiSpam, Content Filters, Stateful Packet Inspection
- Intrusion Detection and Prevention
- Secure Remote Desktop for remote administration
- Monitor SLA of VPN & WAN links (bandwidth/uptime)

VPN Features	PPTP	IPSec	SSL VPN*
Ease of use	Medium	Hard	Easy
Encryption	Poor	Good	Good
Client required	No; Windows has built-in client	Depends on peer service	Yes
Site-to-site VPN	No	Yes	Yes
Client-to-site VPN (road warrior)	No	Yes	Yes
Concentrator failover setup	Medium difficulty	Very difficult	Easy
Concentrator load-balancing setup	Medium difficulty	Very difficult	Easy
Multi-homed concentrator	Yes	No	Yes
Multicast traffic	No	No	Yes
Bridged interface	Yes	No	Yes
Routed interface	Yes	Yes	Yes
Certificate based authentication/PKI	No	Yes	Yes
Password authentication/PSK	Yes	PSK	Yes
Works over NAT	Yes	May not work with all IPSec peers	Yes
Works with dynamic IP	Yes	No	Yes

* ELINA Recommended