

VPN Firewall

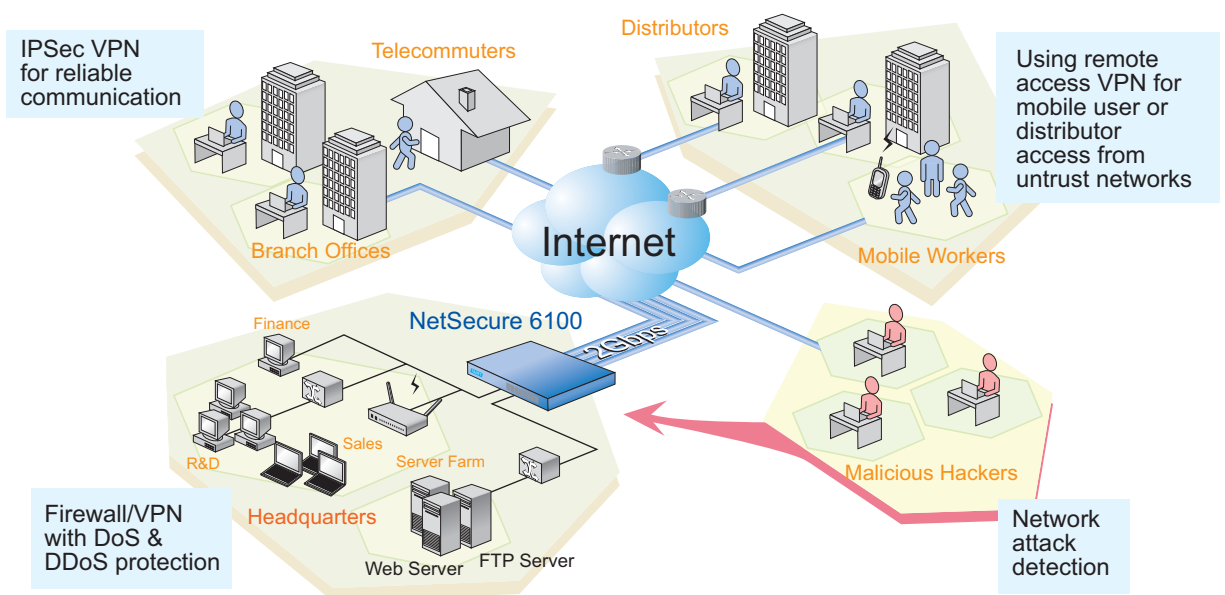
NetSecure 6100

- 2 Gbps+ Hardware-accelerated IPsec VPN
- 2 Gbps+ enhancement firewall function
- Simplified security policy management
- Advanced NAT function including one to one NAT, many-to-one NAT, many-to-many NAT
- High performance DoS and DDoS prevention
- Transparent-mode capability allows seamless integration into most existing network topologies



Today's networks provide a key element infrastructure for fast moving business processes. With more and more incidence of intruders attack on information asset. It shows most of the business networks are exposed under the unsafe environment. TAINET provides the new secure system that will bring your business to the next era.

TAINET NetSecure 6100 is a high performance network security appliance designed for carrier-grade. The NetSecure 6100 integrates DoS and DDoS prevention, IP fragmentation, IPsec VPN, and core IP service into a single platform, with intelligent classification and traffic processing for multi-Gigabit throughput at all packet sizes. Eight fully configurable gigabit Ethernet interface that can be used for LAN, WAN, and DMZ. In addition, NetSecure 6100 also supports IPsec, and L2TP protocols in Client/Server mode and can handle pass-through traffic as well. Advanced VPN configuration options include: DES/3DES/AES encryption, Manual or IKE key management, MD-5 and SHA-1 authentication.



NetSecure 6100

Maximum Performance and Capacity

- Firewall Performance: 2 Gbps
- 3DES/AES performance: 2Gbps
- Concurrent sessions: 500,000
- New session/second: 15,500
- Policies: 24,000
- Interfaces: 8 x 10/100/1000 BaseT

Mode of Operation

- Layer 2 mode (transparent mode)
- Layer 3 mode (route and/or NAT mode)
- NAT (Network Address Translation)
 - One-to-one NAT
 - Many-to-one NAT
 - Many-to-Many NAT
- PAT (Port Address Translation)
- Policy-based NAT
- Virtual IP
- Mapped IP
- Unrestricted Users supported

Firewall

- Number of network attacks detected: 31
- Network attack detection
- DoS and DDoS protections
- TCP reassembly for fragmented packet protection
- Malformed packet protections
- Protocol anomaly
- Stateful protocol signatures

VPN

- Up to 20,000 bi-directional, site-to-site and remote access VPN tunnels
- DES (56-bit), 3DES (168-bit) and AES 256bits
- MD-5 and SHA-1 authentication
- Manual Key, IKE
- PKI (X.509)
- Perfect forward secrecy (DH Groups)
- Prevent replay attack
- Remote access VPN
- IPSec NAT Traversal
- VPN tunnel monitor
- VPN client pass through

Firewall and VPN User Authentication

- Built-in (Internal) database
- 3rd party RADIUS user authentication
- XAUTH/VPN authentication

Logging/Monitoring

- Syslog multiple servers (External, up to 2 servers)
- Email Alerts (2 addresses)
- SNMP (v2)
- Traffic Counters

Routing

- RIPv1/v2 dynamic routing
- Static routes

High Availability (HA)

- Active/Passive
- Configuration synchronization
- Device failure detection
- Link failure detection
- Encryption of HA traffic

IP Address Assignment

- Static
- PPPoE Client
- DHCP Relay

System Management

- WebUI (HTTP and HTTPS)
- Command Line Interface (console)
- Command Line Interface (telnet)
- Command Line Interface (SSHv2.0)
- All management via VPN tunnel on any interfaces
- 3 stored software images

Administration

- Local administrators database
- Admin and Read Only user levels
- Software Upgrades (TFTP, HTTP, HTTPS)
- Configuration Roll-back

