

Introduction

Stealth Networks is a pioneering developer and provider of next generation VPN (Virtual Private Network) and network security solutions. Built with a "security first" philosophy, our integrated solutions provide customers with VPN, firewall, and IPS (Intrusion Prevention System) capabilities far superior to the current industry leaders at a fraction of their cost.

Stealth Networks provides 'easy-to deploy' software and hardware VPN products as well as "fully-managed" VPN and critical network security services.

The Need

As performance demands on silicon based solutions increase, microprocessor and flash memory chip designs become more complex. To produce silicon chips that match these complex design specifications, manufacturers need sophisticated, state-of-the-art equipment which is expensive. Maximizing overall equipment efficiency (OEE) for these capital intensive tools is critical for reducing costs and increasing profits. Hence, every chip manufacturer wants to minimize equipment downtime and mean time to repair (MTTR).

Since semiconductor processing and metrology equipment is complex, the biggest hurdle to minimal downtime and MTTR is the lack of real-time expertise in the factory. On-site experts are very expensive, not always available, and can be overwhelmed by conflicting priorities. e-Diagnostics and similar applications can provide on-demand, real-time expertise at any location. However, the secure deployment of remote diagnostic and repair applications presents many challenges.

One of the major challenges is the availability of a secure and reliable, high performing, data transfer solution that can bridge numerous, disparate supplier networks. For the remote diagnostic applications to provide value, they need to securely transfer large amounts of data between the affected tool and the remotely located tool expert. In most cases, this data is highly sensitive and proprietary. The loss or theft of information can have serious cost and liability implications. Additionally, building a network connecting multiple OEM manufacturers involves dealing with multiple network access technologies and architectures.

To realize the full benefit of e-Diagnostics and similar applications, semiconductor manufacturers require an access agnostic, Internet-based, reliable data transfer solution that can securely transport large quantities of data with minimum overhead while integrating a diverse network infrastructure.

Why Stealth Networks?

Stealth Networks' Secure VPN solution enables semiconductor manufacturers and their partners to securely and reliably share large amounts of data over the Internet. The application neutral Stealth solution works with multiple Internet access technologies and seamlessly integrates with existing network infrastructure. With minimal setup requirements and mobile functionality, the Secure VPN solution outperforms other products in high-volume data transfer environments. Our customers achieve higher bandwidth utilization, lower latency at a low TCO through the following features of our Secure VPN solution:

Best-in Class Security

- No external visibility to your private network
- TLS / SSL supported certificate based authentication with PKI compatibility
- AES 256 encrypted VPN with keys rotated every 60 seconds - the strongest encryption legally available
- Advanced firewall features that restrict buffer overflows, TCP collisions and data leaks
- Powerful Stateful Packet Inspection (SPI), DoS protection and complete IP NATing
- IPS "deny all" approach that blocks all malicious traffic through dynamic rule set loading

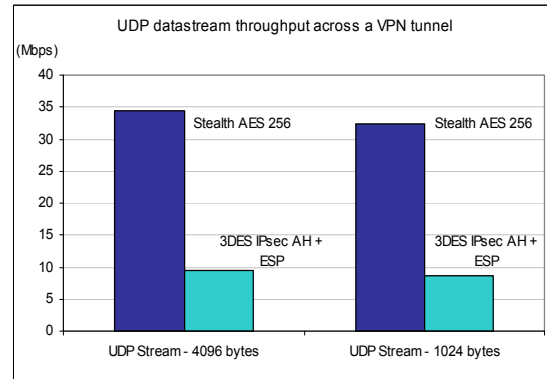
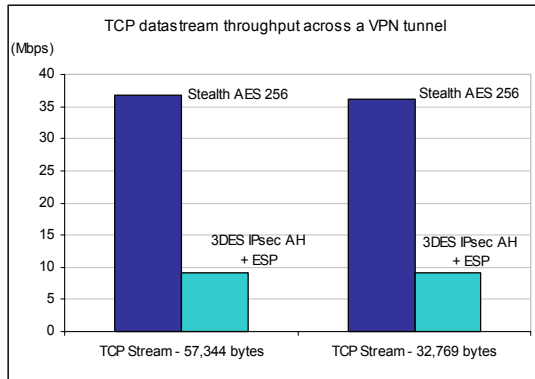
Enhanced Productivity and Cost savings

- Plug-and-play deployment, seamless integration with existing network infrastructure
- Reliable and scalable open specification hardware - reduced equipment costs
- End-user transparent, reduced support costs – lower TCO

Stealth Networks

Superior Performance & Control

- 3-4X more encrypted data throughput at higher encryption levels (refer graphs below)
- Granular access management and control
- Fine-grained auditing and logging
- Multi-homing, active failover and clustering capabilities



Stealth Secure VPN Architecture

Stealth Networks' VPN solution can be deployed in site-to-site, remote access or a hybrid model. Site-to-site VPNs require Stealth Secure Gateways at each location while mobile secure access is enabled through a Stealth Software VPN client.

Stealth Networks' Secure VPN can be deployed in either of the two architectures described below. If required, a hybrid architecture in-between these two extremes can also be deployed.

- Hub and Spoke topology with "force-all tunnel" configuration - In this scenario all traffic from remote sites is forced into the VPN tunnel to the host / main site. Access between any two remote sites as well as Internet access for all sites is routed through the host site.
- Full Mesh topology with "split tunnel" configuration - In this scenario all sites can communicate with each other directly without going to the host / main site. Independent Internet access is also provided for each site.

Stealth Networks Secure VPN Architecture

