GlobalDAT™

GLOBAL DIRECT ACCESS TRADING SYSTEM

TECHNOLOGY DESCRIPTION

GlobalDAT™ is a proprietary direct access trading system, that provides real-time quotes and order-entry to multiple US and European markets. All our connections, software, APIs, and infrastructure is proprietary and developed in-house. We access all markets real-time with dedicated connections and code without any intermediary. We always install our software directly with a particular Stock Exchange member, ECN or settlement agency, and by utilizing order validation and risk-management systems based in our European co-location, we link all these Stock Exchanges and interfaces together, thus providing secure and super-fast environment for your GLOBAL trading. Global settlement account, using multiple currencies, is provided by Penson Worldwide, Inc. and complements our system, making GlobalDAT™ the only truly Global Direct Access trading solution.

APIs supported:

US markets:

- NASDAQ SOES
- NASDAQ SelectNet
- NYSE / AMEX
- Island ITCH / OUCH
- ARCA
- GNET (OTC-BB)
- OATS
- Penson US, Dallas, settlement interface

Worldwide markets:

- Omiris, Inc. interface through FIX 4.2 engine, offering links to 30 Stock Exchanges (Euronext, Australia, Brazil, Denmark, Hong-Kong, India, Italy, Japan, South Africa, Canada, Norway, New Zealand, Russia, Taiwan, Thailand)
- London Stock Exchange API (StockAcademy being an executing broker)
- Xetra Germany API (Peter Koch eXchange being an executing broker)
- Penson Worldwide (UK) interface

Hardware we use (see later sections for technology, security and availability details):

- Sun 3800 mainframe computers
- Sun Netra T1 quotes servers
- Sun Netra X1 application servers
- Cisco 7200 routers
- IPSec cards
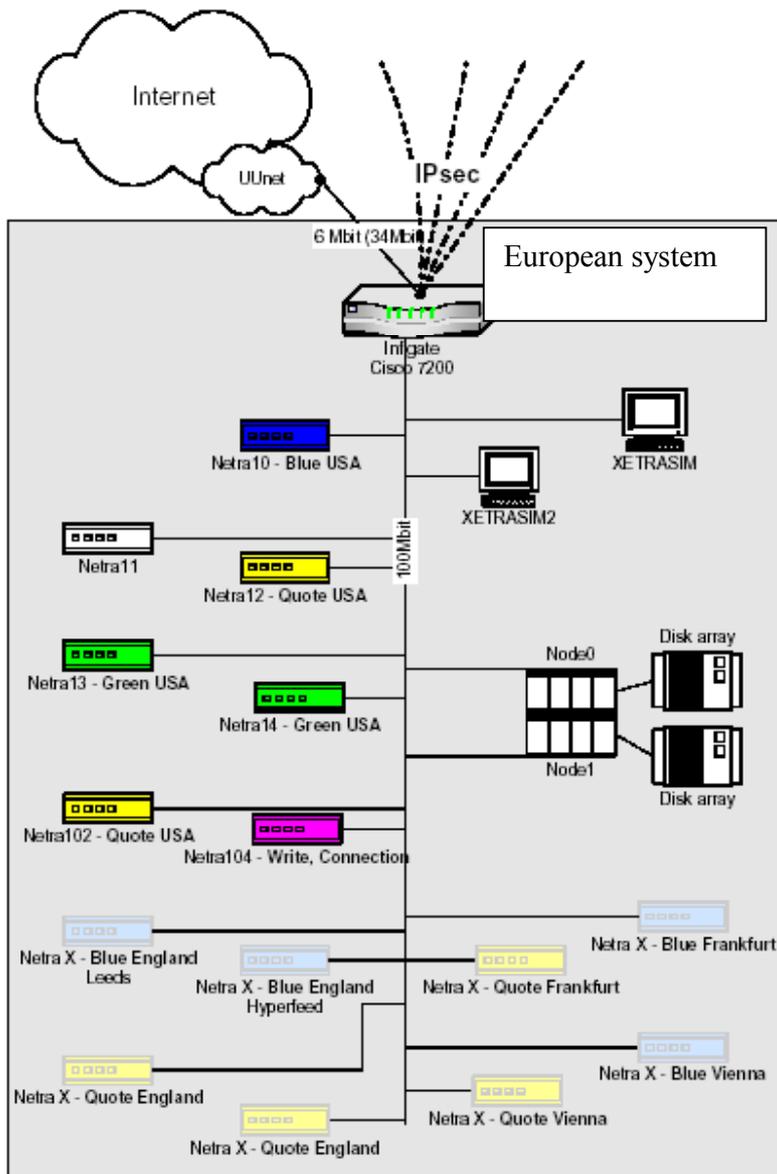- Dell Precision workstations for administration

Development tools:

- Sun *Solaris 8* operating system on all production-environment computers
- Utilizing *Sun Forte C++* for all application servers
- *Oracle 8i* database running on Sun Solaris 8, using *PL/SQL* procedures and functions
- Front-end coded in *Borland Delphi 6* and *Borland C++ Builder 6*
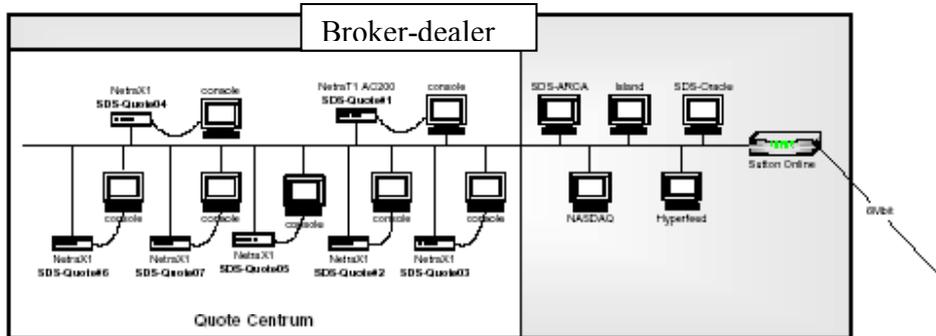
Development and testing environment:
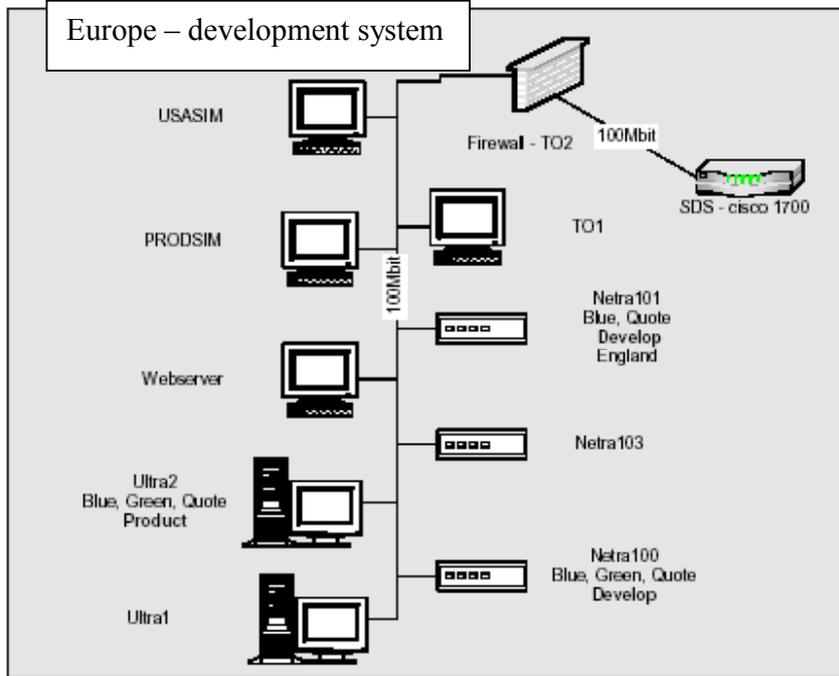
This is the development system that we test, stress-test and develop all APIs on. It is not directly related to any of 2 production-run co-locations, but it is necessary to emphasize that we are using the same computers, hardware and software configuration in both develop and production environments to ensure that our systems run 100% on time and there are no incompatibilities. In case both production co-locations would fall-down, which is an extremely unlikely event, all traffic could be re-routed within 1 minute to our development system.

Production system 1: co-location EUROPE

Production system 2: co-location USA

HW configuration used:

GlobalDAT security

GlobalDAT system utilizes public network, Internet, as a transfer medium, so all transfers between the particular nodes of our network are ciphered, including one development, and two production co-locations. The transfers between the European center, connected brokers and US quote centers are secured by IPSec protocol and by the Triple DES cipher. The transfers between the clients and our centers are secured by industry standard SSL protocol..

• **IPSec**---IP Security Protocol. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

• **Internet Key Exchange (IKE)**---A hybrid protocol which implements Oakley and SKEME key exchanges inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys.

• **DES**---The Data Encryption Standard (DES) is used to encrypt packet data. Cisco IOS implements the mandatory 56-bit DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet. For backwards compatibility, Cisco IOS IPSec also implements the RFC 1829 version of ESP DES-CBC.
• IPSec supports the **Triple DES** encryption algorithm (168-bit) in addition to 56-bit encryption. Triple DES (3DES) is a strong form of encryption that allows sensitive information to be transmitted over untrusted networks. It enables customers, particularly in the finance industry, to utilize network layer encryption.

IPSec Transport and Tunnel Modes

IPSec can be configured in tunnel mode or transport mode. We use the tunnel mode. In IPSec tunnel mode, the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPSec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPSec tunnel. The destination router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to receive the benefits of IPSec. Tunnel mode also protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints. In IPSec transport mode, only the IP payload is encrypted, and the original IP headers are left intact. (See Figure 5-1.) This mode has the advantage of adding only a few bytes to each packet. It also allows devices on the public network to see the final source and destination of the packet. With this capability, you can enable special processing (for example, QoS) on the intermediate network based on the information in the IP header.

However, the Layer 4 header will be encrypted, limiting the examination of the packet. Unfortunately, by passing the IP header in the clear, transport mode allows an attacker to perform some traffic analysis.

IPSec in Tunnel and Transport Modes
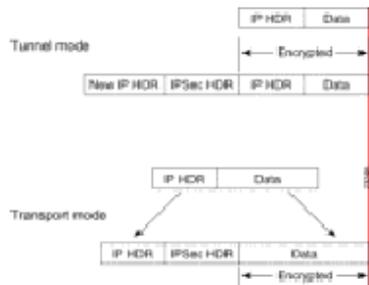
SSL

The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP or IMAP. It uses TCP/IP on behalf of the higher-level protocols, and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection.

Scheme
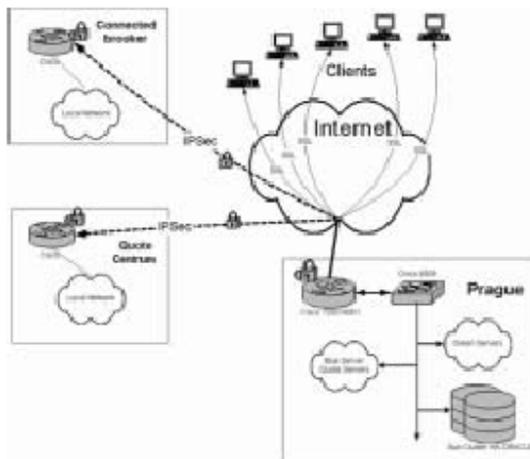
Hardware

High Availability Cluster

The most important parts of our system are operated by High Availability Sun Cluster. Sun Cluster delivers high availability -- through automatic fault detection and recovery – and scalability, ensuring that your mission-critical applications and services are available when you need them. Leveraging and extending the reliability, scalability, and performance of the industry-leading Solaris Operating Environment, Sun Cluster provides mainframe-class reliability, availability, and scalability. A cluster is a group of nodes that are interconnected to work as a single, highly available and scalable system. A node is a single instance of Solaris software – it may be a standalone server or a domain within a standalone server. Sun Cluster scales up to 256 processors in a cluster -- enough to handle growing numbers of simultaneous users and access to large databases. With Sun Cluster, we can add or remove nodes while online.

High Availability

With Sun Cluster software installed, other nodes in the cluster will automatically take over and pick up the workload when a node goes down. It delivers predictability and fast, agile recovery capabilities through features such as local application restart, individual application failover, and local network adaptor failover. Sun Cluster significantly reduces downtime and increases productivity by helping ensure continuous service to all your users.

Performance/Scalability

With Sun Cluster software, we can cluster up to four nodes to meet the performance and manageability needs of our data center. By allowing an application to scale across multiple servers in this manner, Sun Cluster delivers increased performance and throughput.

Investment Protection

Sun Cluster provides the scalability to grow with our business, protecting our investments in Sun servers and storage systems. Our network can start with a standalone server, and as the need for higher availability or scalability develops, we can cluster domains within that server. As our business grows, we can easily add new servers to the cluster for increased service capabilities.

Flexibility in Integration

Sun Cluster supports the dynamic addition or removal of nodes, and enables Sun servers and storage products to be clustered together in a variety of configurations. Existing resources are used more efficiently, resulting in additional cost savings.

Telehousing

Our hardware is placed in the Telehotel of Infigate company for co-location 1 (Europe) and AT&T for co-location 2 (USA, New York).

Security Concept

An active access control system (encoded card system) protects INFIGATE Telehotels against unauthorized access. A PC-based authorization system enables the customer to make short-term changes (e.g. over the phone) in the access authorization of his staff. A 24-hour security personnel completes the access control by constantly monitoring – via video cameras – any activities and movements within the Telehotel. In addition, our Telehotels are equipped with an automated alarm system, which will signal intrusion (burglary), sabotage, raids, smoke detection, fires as well as malfunction of building systems.

Double Floor

The telehousing rooms of our Telehotels are equipped with a 600 mm double floor, which can carry loads of up to 500 kg / m². The customer is responsible for observing this maximal load and will be held liable in case of damage. The double floor has a number of openings for air-conditioning of system cabinets as well as power supply and data cables.

Secure Power Supply

Telehotel is equipped with a secure power supply, which provides 230 Volts/AC and 48 Volts/DC without interruptions, based on large-sized DC accumulators and an emergency unit. Availability of power supply is at least 99.99% per operational year and is covered by a service commitment. The maximum electrical power consumption for all connected devices, which is binding for the customer, depends on the volume of his service contract (product, quantity). Should the customer require extra amounts of electrical energy, this has to be agreed with INFIGATE and, if appropriate, will be invoiced separately.

Controlled Room Air Conditions

Telehotel is equipped with sophisticated room air conditioning and heating systems, which will ensure an optimum room temperature according to ETS 300 019-2-3 Class 3.1. Additional ventilation systems with air filters as well as an air humidity control system ensure appropriate air conditions.