Sun™ Secure Global Desktop Software

Security Considerations
White Paper

August 2006

Table of Contents

Sun Secure Global Desktop Software from a Security Perspective

One of the key weaknesses of current approaches to corporate desktop computing is that of a weak informational security model. In many organizations intellectual property (IP) in the form, for example, of sensitive documents or source code, can leak out across a user community with little or no access control or audit capability. Against a backdrop of increasingly demanding industry and government compliance rules this presents a real problem to many organizations. The challenge being addressed is how do we protect the data most valuable to the business without constraining the agility or efficiency of the business?

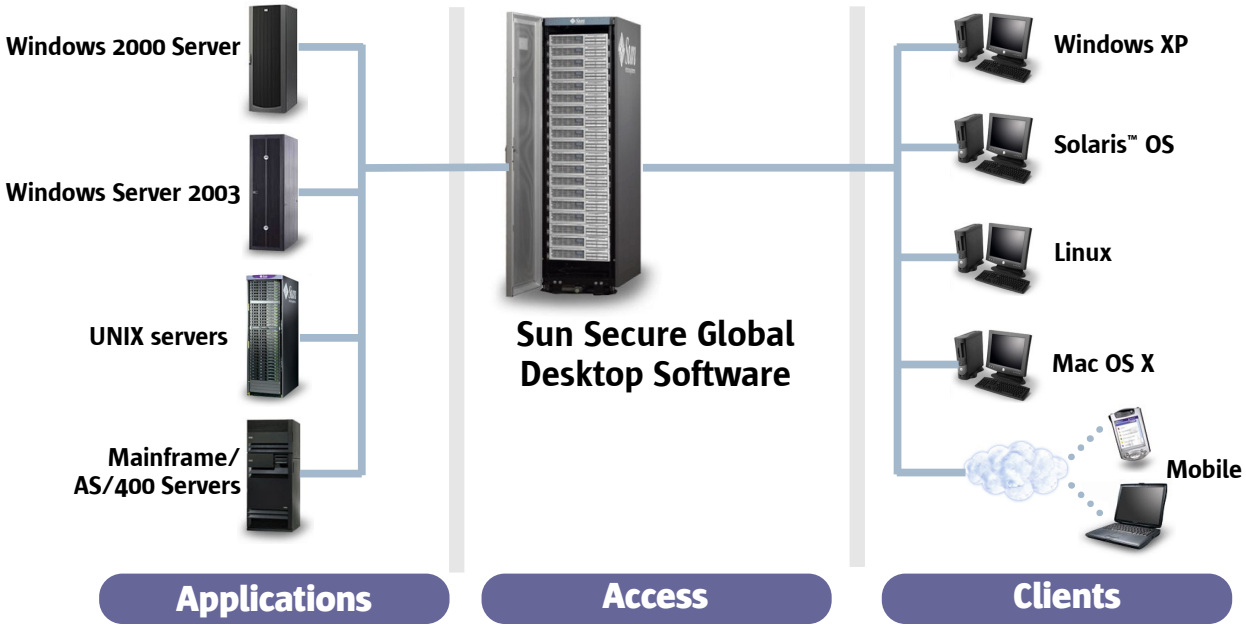
A potential solution to this problem is one which would allow the IP to remain in a secure and managed location, such as the corporate data center, but allow controlled access to this information by people authorized to use it. This server-based approach is the one provided by Sun Secure Global Desktop Software.

But how secure is this system? Is any organization really going to trust making their business critical information and applications available beyond their organizational boundaries unless there is trust in the security of this model?

This white paper outlines the functionality of Sun Secure Global Desktop Software from a security perspective. We will look initially at what the product does before drilling into how it does it.

Basic Architecture

Sun Secure Global Desktop Software uses a powerful 3-tier architecture to provide universal access to virtually all desktop applications, including those that run on Microsoft Windows, UNIX®, Linux, mainframe or midrange servers.



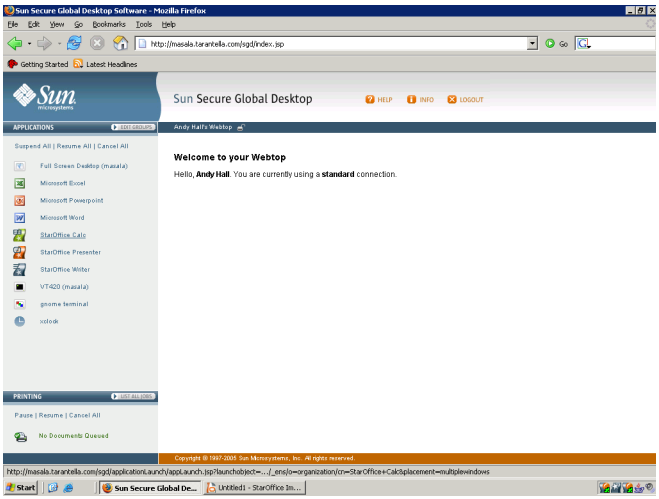
- The Applications Tier - Applications run on centrally managed application servers. These servers can consist of machines dedicated to one operating system, machines running multiple operating systems using virtualization technology, or a mixture of the two.
- The Access Tier - Sun Secure Global Desktop Software is typically hosted on one or more dedicated Sun Solaris OS or Linux servers where all information about users and applications are held. Sun Secure Global Desktop servers can be joined together into an “array” for scalability reasons while retaining a single administration point.
- The Client Tier – Popular client devices such as Microsoft Windows PCs, UNIX or Linux workstations, Internet devices, and Windows Mobile-based PDA’s, can be used. For users who don’t have a web browser and for embedded devices, Sun Secure Global Desktop Native Clients are available on many different platforms

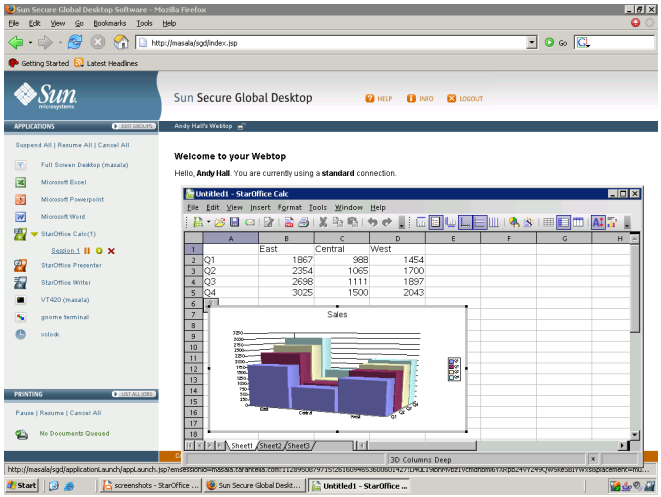
A wide range of connection types are supported, and the Adaptive Internet Protocol (AIP) ensures optimal performance over complex network routes with varying bandwidths. AIP employs heuristics to determine the type of device and network connection in use, and dynamically adapts to optimize performance.

The User's Experience

The typical user experience is as follows:

- The user points their web browser or Secure Global Desktop Native Client at the URL of the Sun Secure Global Desktop Software server. E.g. https://*servername*/sgd
- For users using a browser, the Sun Secure Global Desktop Client is securely downloaded as a signed Java™ archive and executed. The download only happens on the first connection to the server, subsequent connections will not involve an archive download.
- The client then connects back to the Sun Secure Global Desktop Software server and the user is prompted to authenticate.
- The user enters credentials which the server validates against a choice of authentication mechanisms
- When authentication is successful, the user is presented with her "webtop" containing a list of applications that the administrator has published to her.
- To launch an application, the user simply clicks on an application icon.
- The user can use the application as though it were running on their local PC. She can copy and paste between local and remote applications, print to local printers and even access the file system of the local client from the 3rd tier applications if the administrator has allows this.
- All communication between 1st and 2nd tier may optionally be SSL encrypted although the user is unaware of this.





Security Overview

In order to examine the security precautions of Sun Secure Global Desktop Software, let us imagine a hostile scenario as follows.
The application servers are located on the internal network protected by 2 firewalls with the Sun Secure Global Desktop array located in the DMZ (De-Militarized Zone). Clients are assumed to be beyond the external firewall although in reality they may be within another organization's network. Both the clients and the Sun Secure Global Desktop servers are therefore in extremely hostile environments and the Sun Secure Global Desktop Security Pack is installed on the array.

The following walk-through describes precautions taken at each stage of operation.

Assets and Threats

The “assets” that Sun Secure Global Desktop Software is protecting are:

1. access to the applications and the data the applications use; and
2. the data in transit between the Sun Secure Global Desktop client and the server.

Threats to these assets include unauthorized access or users exceeding their authority.

Delivery of the client

The first attack in this hostile scenario could come during the process of downloading the Sun Secure Global Desktop client to the client device. To protect against this, it is recommended that only HTTPS connections be used to connect to the Sun Secure Global Desktop server. Downloading over HTTPS ensures that the browser can verify that the server really is the genuine server and that the data cannot have been tampered with. Finally, the Java client archives from Sun Secure Global Desktop are digitally signed using code-signing certificates from Verisign to further prove authenticity.

Proxy Server detection

Some deployments may use proxy servers en-route to the Internet. The Sun Secure Global Desktop clients can detect and work with proxy servers, also allowing for authenticating proxies if used.

Server authentication

The next stage is for the Sun Secure Global Desktop client to connect to the server. By requiring the Sun Secure Global Desktop server to provide an X.509 server certificate, the Sun Secure Global Desktop client can be sure that the URL it is connecting to is truly who it claims to be and that there is no man-in-the middle of the conversation. Also at the stage Sun Secure Global Desktop Software supports client-side web-proxy servers including authenticating proxies which are used in some organizations before a client can reach the Internet.

Client IP Filtering

Sun Secure Global Desktop Software can make decisions about the type of connection allowed based upon the IP address of the client. The decision can be to:

1. Insist upon an SSL connection
2. Allow a standard connection
3. Deny a connection altogether

Ranges or distinct IP addresses are permitted. A typical use is to allow standard connections from IP addresses on the

LAN but insist upon SSL connections from all other addresses, or to simply deny from unexpected addresses.

User Authentication

Having established a secure tunnel between client and server, only then is the user allowed to attempt to log in to the Sun Secure Global Desktop array. The user submits their credentials and Sun Secure Global Desktop Software checks these against one or more login authorities, or 3rd party authentication systems. These include:

- LDAP and Secure LDAP (including Microsoft Active Directory and the Sun Java™ Enterprise System Directory Server.
- Windows NT or Windows 2000 domain
- RSA ACE/Server (for RSA SecurID two-factor authentication)
- UNIX user database (including NIS)

Administrators have full control over which login authorities are in use across the array. For more details of the login authority mechanism see the product documentation, which is also available on the Sun web site. Additionally, Sun Secure Global Desktop Software can optionally prohibit users from logging in if they exceed a maximum number of attempts.

In addition to the built-in authentication types, Sun Secure Global Desktop Software can support web-server authentication. In this mode, access to the Sun Secure Global Desktop URL can be protected using the web-server mechanisms which may include HTTP Basic authentication, but in our hostile environment here, is more likely to use strong authentication such as client certificate or other 2-factor solutions from companies such as Secure Computing, Netegrity or RSA Data Security. This is often used in scenarios where a corporate standard is in use for accessing resources over http(s).

Access Control

Assuming that a valid user has been able to login, the user will be sitting at their webtop showing the list of applications they can run. In Sun Secure Global Desktop Software, these are the only objects that a user can run. This is deliberate and assists in protecting against the threat of users attempting to exceed their authority.

Application server authentication

To run an application from their webtop, users must log in to the application server that hosts the application. Sun Secure Global Desktop Software presents the user with the appropriate authentication dialog for the type of application server, and forwards the credentials to the application server. The Sun Secure Global Desktop array maintains a secure application server password cache, which can store user credentials if the security policy of an organization permits this. If credentials are already cached for a user when they run an application, they're passed automatically to the application server and the user isn't prompted.
Administrators can use administration tools to add, edit and remove entries from the password cache.
Sun Secure Global Desktop Software includes support for application server password expiry, and where possible allows the user to change their password if the application server indicates it has expired.

Secure Transmission

So, by now, a user has logged in and launched the application. To ensure that the traffic on the wire cannot be eavesdropped, the Sun Secure Global Desktop Security Pack uses SSL v3 and TLS to deliver up to 256-bit strongly encrypted connections between the client and the Sun Secure Global Desktop server. The cipher suite uses RSA for key exchange and AES-256 for bulk transfer with a SHA-1 hash.

Secure connections to application servers

It should not be forgotten that the DMZ is a hostile environment too and the connections between the Sun Secure Global Desktop server and application server should also be encrypted. For UNIX and Linux applications Sun Secure Global Desktop Software can use SSH to provide secure communication, whereas for connections to Windows servers, an encrypted RDP stream is used (FIPS-level encryption is not supported).

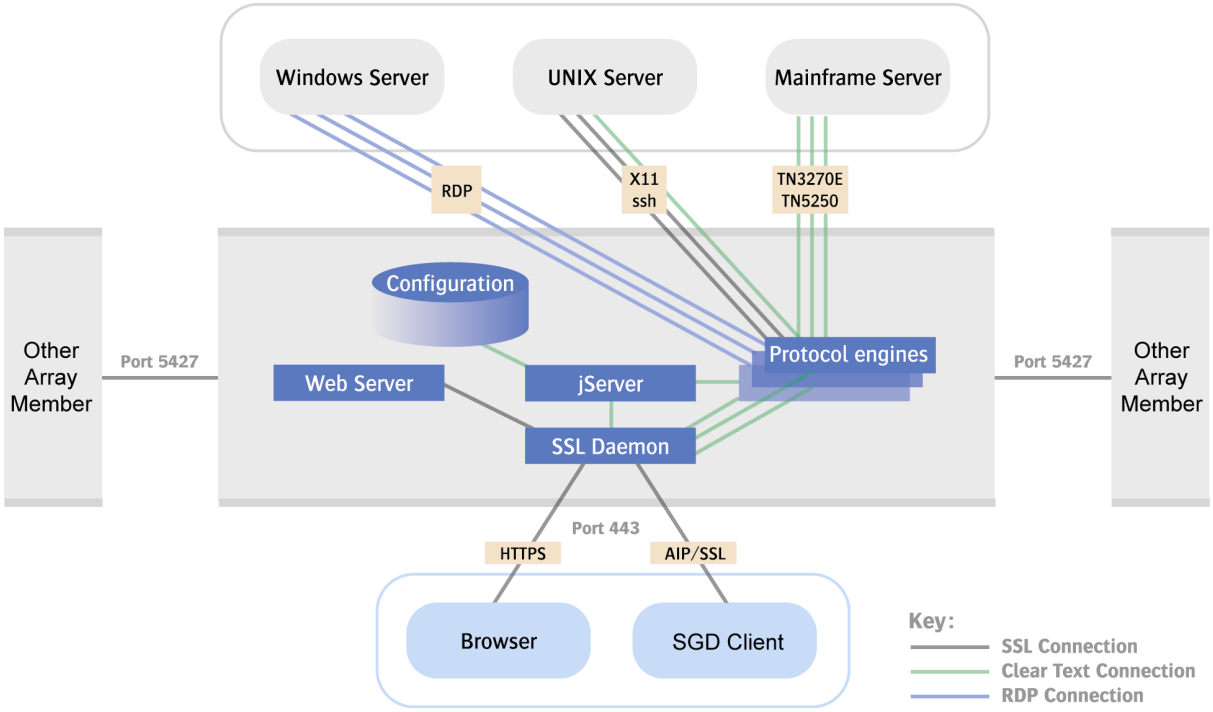
Auditable Access

Sitting between users and applications, Sun Secure Global Desktop Software is uniquely positioned to log all activity including who did what, when, and for how long. Because of this, Sun Secure Global Desktop Software can provide detailed audit trails of information, including failed login attempts.
Secondly, any configuration changes are also recorded and logged.

A Secure Architecture

A final key point in Sun Secure Global Desktop Software ’s security story is that of the architecture itself. Application servers are never exposed to direct connections from clients on the Internet. Secondly, the Sun Secure Global Desktop server platform is usually Linux or UNIX, platforms which are renowned for reliability and security and often trusted to DMZ deployments.

Components and Connections



Web server

Sun Secure Global Desktop Software includes the Apache web server and the Tomcat Servlet engine, collectively referred to here as the web server.

The web server binaries are installed as part of the 'Base Component'.

For customers who prefer to use their own web server, it is possible to disable it and substitute it with another web server such as the Sun Java Enterprise System web server for instance.

The web server is initially used to deliver the Secure Global Desktop Client itself and configuration to the client.

Secondly, the web server can be used for authentication (see User Authentication above).

Finally, Sun Secure Global Desktop Software includes several web applications, which look after presenting the user's webtop and handling the launch of applications, as well as some administration utilities.

The Client Component

The Client Component has 3 main forms:

1. The browser-based client (TCC) which is used when the /sgd URL is used. This is delivered as a signed Java archive and contains a mix of Java and native code components.
2. The Classic client is a different Java archive which consists mostly of Java and a few native helper executables. It is used when the user visits the /tarantella URL. It is deprecated and Sun recommends customers use the more modern TCC which makes better use of the server for tasks such as the webtop presentation.
3. The Native Client is a standalone executable which does not use a browser. It is typically used when a browser is not present or not desired. Native Clients are available for Windows, Solaris OS (SPARC® Platform Edition) and Solaris OS (x86 Platform Edition), RedHat Linux, SuSE Linux, Windows Mobile (PocketPC), Mac OS X, as

well as for Linux and other UNIX platforms.

When operating with the Sun Secure Global Desktop Security Pack, the client is responsible for the client-side SSL connection and it makes the initial connection. Sun makes use of the widely regarded OpenSSL technology for this. The client is told which port on the Sun Secure Global Desktop server to make AIP connections to by an initial HTTP(S) conversation with the web server.

Web Servlets

Sun Secure Global Desktop Software makes use of a series of servlets to display a variety of information such as the user's webtop content, application launch, printer status, and diagnostic information. Some servlets are designed for administration of the system and are only available to Administrators.

SSL daemon

The SSL Daemon is the server-side component responsible for the SSL/AIP conversation that takes place between the Sun Secure Global Desktop client and the server. SSL encryption is implemented using the OpenSSL toolkit. The SSL daemon is installed as part of the Sun Secure Global Desktop Security Pack. A Sun Secure Global Desktop Software installation that does not run the Sun Secure Global Desktop Security Pack uses unencrypted connections between the clients and the Sun Secure Global Desktop server.

The SSL daemon runs on port 5307 by default, however to support firewall tunnelling it can be configured to use port 443. In this configuration, the HTTPS server is moved to say, 127.0.0.1:443 while the daemon sits on the public port. The daemon receives both HTTPS and SSL/AIP traffic. It deals with SSL/AIP traffic directly but forwards HTTPS traffic on to the HTTPS server.

The key used is held and protected by the file system.

JServer/Proxy server/Datastore

These components form the core part of the Sun Secure Global Desktop Software server. They are responsible for authenticating users, accessing the Datastore and generating the list of published applications, handling the application launch, load distribution, managing the print queues, managing sessions and synchronization throughout an array.

The Datastore contains information about applications, application servers, and possibly also users. This information is held in the file system and relies on the files ystem for protection of this.

Protocol Engines

Protocol Engines are server-side emulators that understand the application server protocols (RDP, X11, etc). In essence they appear as “clients” to the application server. The screen content of the application sessions is virtualized and transmitted over the Sun Secure Global Desktop Adaptive Internet Protocol to the Sun Secure Global Desktop clients. When the Sun Secure Global Desktop Security Pack is being used the Protocol Engine talks over a local socket to the SSL Daemon who performs the encryption before transmission. User input sent by the client arrives in the reverse direction, via the SSL Daemon if the Sun Secure Global Desktop Security Pack is being used.

Launch Engine and Password Cache

The Launch Engine makes connections to the application servers. Depending on the application server type, this may invoke the use of scripts to authenticate a user to an application server or, as part of protocol, pass credentials to the application server.

For UNIX/Linux application servers the scripts use Expect/Tcl whereas for Windows applications the Microsoft RDP Protocol is used.

The third tier or application server credentials are held in the Password Cache. This is indexed by the username used to login to the Sun Secure Global Desktop Server and provides a transparent login process for users.
The cache is held in an encrypted form on disk using a 168-bit 3DES algorithm and a key that is generated when the Sun Secure Global Desktop server starts up. The key can be regenerated when the Sun Secure Global Desktop server restarts or may be persistent across server instances. In both cases, the key is stored and protected by the file system. Administrators can manipulate the password cache using the “tarantella passcache” command line utilities or may choose to disable the caching of passwords altogether.

Inter-Array Traffic

Nodes in the Sun Secure Global Desktop Array communicate with each other over port 5427. This traffic is used to maintain a “single system image” of the states of each node in the array. This data is also encrypted using the default cipher suite which uses RSA-AES256-SHA1.

Dealing with Vulnerabilities

Sun Microsystems operate a public security alert newsletter which is published weekly and contains information on known security vulnerabilities or weaknesses. To subscribe to this newsletter please visit http://sun.com/newsletters/

The Overall Security Regime

Sun Microsystems, Inc. take the security of our customers networks very seriously and make every endeavor to deliver secure products. However, it should be noted that the security features of Sun Secure Global Desktop Software software and the Sun Secure Global Desktop Security Pack are intended to be used in conjunction with, and not as a replacement for, standard security practices.

For example, Sun Secure Global Desktop Software contains no explicit functionality to deal with Denial of Service attacks but rather would expect these to be handled by another entity in the overall security architecture.

Related Links

See the following resources for further information:

For the latest information about Sun Secure Global Desktop Software , see the website at http://www.sun.com/software/products/sgd/