

LESSON OBJECTIVES

- Understand how Secure Global Desktop supports proxy servers
- Configure multiple external DNS names for an array
- Configure Secure Global Desktop to work through firewalls

13

13 Firewalls and proxy servers

13.1 CONCEPTS

Firewalls can separate different parts of your network infrastructure, to restrict network traffic between them. Tarantella Secure Global Desktop Enterprise Edition requires certain firewall holes to be present to work, but the *firewall traversal* feature can be used to grant access in the most typically restricted environments, even those over which your organization has no control.

Secure Global Desktop supports firewalls:

- Between client devices and Secure Global Desktop servers
- Between Secure Global Desktop servers in an array
- Between Secure Global Desktop servers and application servers
- Between Secure Global Desktop servers and authentication/directory servers

In addition, Secure Global Desktop supports HTTP, Secure and SOCKS (v5) client-side *proxy servers*.

Secure Global Desktop allows you to use different external DNS names for the same hosts on different networks. For example, a Secure Global Desktop server's external DNS name when accessed from outside a corporate firewall can be different to its DNS name when accessed from inside that firewall.

13.2 PROXY SERVERS

Client-side proxy servers are supported when logging in from a web browser and from a Secure Global Desktop Client, but the level of support differs.

In all cases, a Security license must be installed in the array to allow access through an HTTP or Secure proxy server (this is not required for access through a SOCKS proxy server).

For HTTP and Secure proxy servers, both Basic authentication and no authentication are supported.

For SOCKS proxy servers, both username/password authentication and no authentication are supported.

13.2.1 Web browser clients

When logging in to Secure Global Desktop using a web browser, the browser's proxy settings are detected and used. Secure Global Desktop supports manually configured or automatically configured HTTP, Secure and SOCKS v5 proxy servers.

To use autoconfig files to set a client's proxy server settings automatically, use a JavaScript file with either no extension or the extension `.pac`, and follow the guidelines at <http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html>

See also: *Administration Guide* » *Security* » *Configuring proxy server settings on clients*

The proxy server settings are detected from the browser using code included in the Java archives for Secure Global Desktop.

For troubleshooting, users can go to a special page that displays information about the detected proxy settings. See *Administration Guide » Security » How can users check whether Secure Global Desktop can access their proxy server configuration?*

13.2.2 *Secure Global Desktop Clients*

To use the Secure Global Desktop Client with proxy servers users must manually configure the settings. HTTP and SOCKS v5 proxy servers are supported (but not Secure proxy servers).

Proxy server settings are configured in the *Options* dialog for the Secure Global Desktop Client.

See also: *Administration Guide » Security » Configuring proxy server settings on clients*

13.2.3 *Dropped connections*

Proxy servers usually drop connections that remain idle for a few minutes. If this happens, a user's application disappears unexpectedly (it doesn't exit: the session is suspended).

To resolve this problem Secure Global Desktop sends regular "keepalive" messages. The frequency of these keepalives is configurable to help you deal with proxy servers that are particularly eager to drop connections.

To find out how to configure keepalive frequencies, see *Administration Guide » Applications, documents and hosts » Applications disappear after about two minutes.*

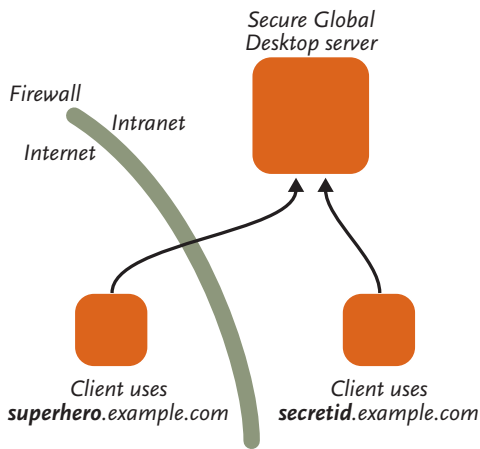


Figure 13-A: Why you might need multiple external DNS names

13.3 EXTERNAL DNS NAMES

A Secure Global Desktop server has one peer DNS name and one or more external DNS names. The peer DNS name is used by other array members; the external DNS names are used by client devices.

You can configure Secure Global Desktop to use different external DNS names for different ranges of clients. You would typically do this if you have a firewall between clients and Secure Global Desktop servers, use different names inside and outside that firewall, and want access from clients both inside and outside the firewall. See Figure 13-A.

In this example we'd want to use two names:

- For intranet clients (with IP addresses 192.168.0.*, say), the name secretid.example.com
- For all other clients, the name superhero.example.com

To set a Secure Global Desktop server's external DNS names in Array Manager, use the *General* properties panel for the Secure Global Desktop server. Here we'd use two lines:

```
192.168.0.*:secretid.example.com
*:superhero.example.com
```

Changes to a Secure Global Desktop server's external DNS names only take effect when you restart the server.

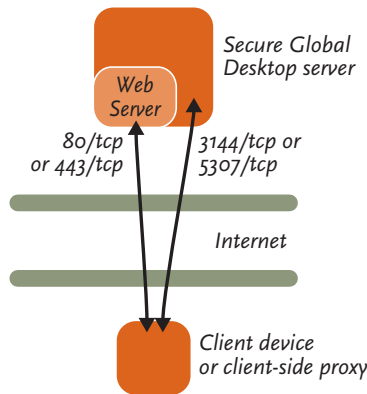


Figure 13-B: Typical firewall configuration between client devices and Secure Global Desktop servers

13.4 FIREWALLS BETWEEN CLIENT DEVICES AND SECURE GLOBAL DESKTOP SERVERS

There may be multiple firewalls between client devices and Secure Global Desktop servers. For example, the client device may be within a LAN that's protected from the Internet by a firewall, and the Secure Global Desktop server may be somewhere on the Internet behind another firewall. Some or all of these firewalls might be outside your control. If Secure Global Desktop-related traffic can't get through the firewalls, users won't be able to log in or access any applications.

Also, each Secure Global Desktop server in an array might be behind a different firewall.

By default, you need access through the appropriate firewalls to two ports on each Secure Global Desktop server in the array:

- 80/tcp for HTTP traffic to the web server (whether the Secure Global Desktop Web Server or any other web server)
- 3144/tcp for unencrypted ASAD/AIP traffic

You may also need other ports:

- 443/tcp for HTTPS traffic to the web server
- 5307/tcp for encrypted ASAD/AIP traffic (using the Secure Global Desktop Security Pack)

If you use only HTTPS and the Secure Global Desktop Security Pack, you don't need to open 80/tcp or 3144/tcp in the firewalls. Typically you would use *either* 80/tcp and 3144/tcp, *or* 443/tcp and 5307/tcp.

Ports 3144/tcp and 5307/tcp are registered with IANA (www.iana.org) and are in principle reserved for Secure Global Desktop-related traffic.

13.4.1 Firewall traversal

You may not have control over all firewalls between clients and Secure Global Desktop servers. Ports 80/tcp and 443/tcp are typically open for HTTP and HTTPS connections, but ports 3144/tcp and 5307/tcp are usually closed.

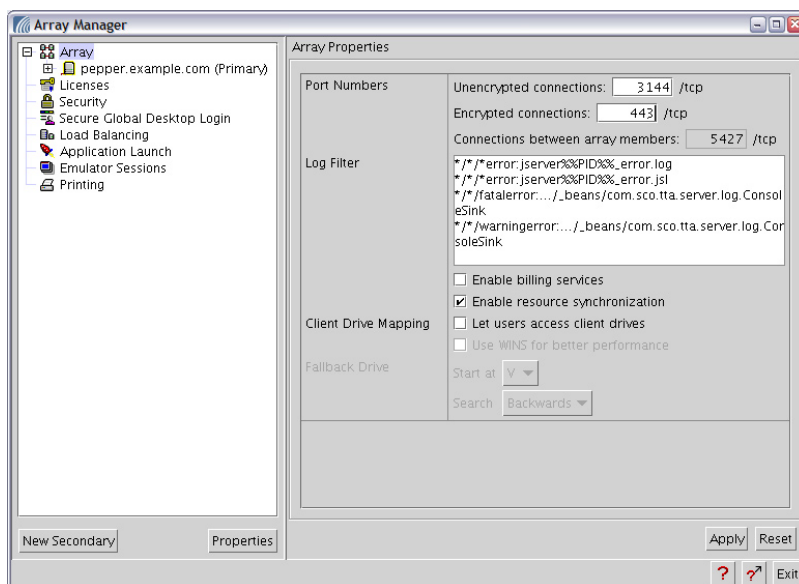
Where it is not possible to open the required ports, you can use the firewall traversal feature to allow full Secure Global Desktop functionality over just one port, typically 443/tcp.

To use firewall traversal, the Secure Global Desktop Security Pack must be installed on each array member and a Security license must also be present in the array.

With firewall traversal, all connections are made over the single port to the Secure Global Desktop server. This then *forwards* all non-ASAD/AIP traffic to the web server on the same host.

To use firewall traversal:

1. Configure Secure Global Desktop to use 443/tcp for its encrypted connections.



In Array Manager, change the *Port Numbers: Encrypted connections* setting on the *Array* panel. This setting applies array-wide.

2. Configure the web server on each array member to bind only to localhost:443.

For the Secure Global Desktop Web Server or Apache, edit `httpd.conf` and change the line:

```
Listen 443
```

to read:

```
Listen 127.0.0.1:443
```

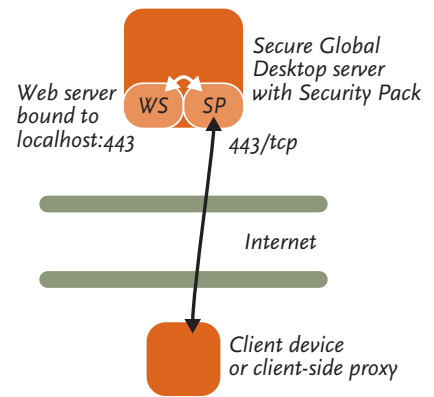


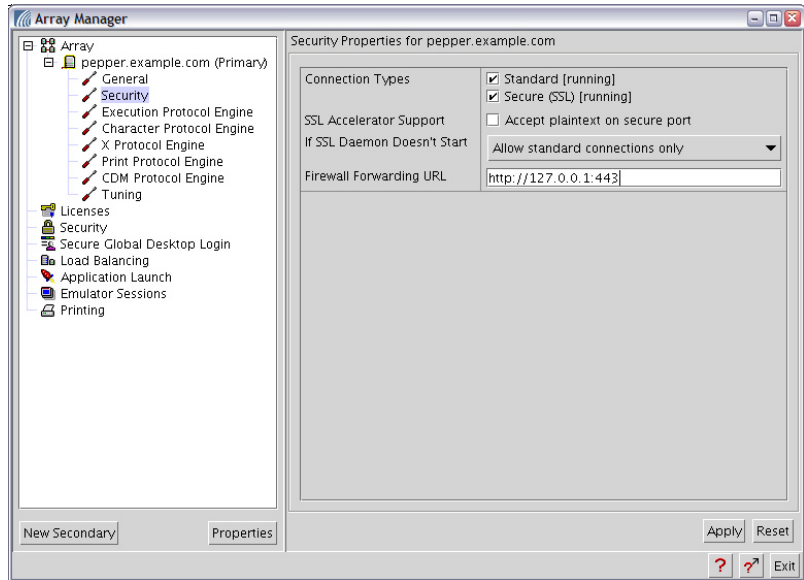
Figure 13-C: Firewall traversal uses a single port for all traffic

Figure 13-D: Changing the port used for encrypted connections

- Configure each Secure Global Desktop server in the array to forward non-ASAD/AIP traffic to localhost:443.

13 Firewalls and proxy servers

Figure 13-E: Changing the Firewall Forwarding URL attribute



In Array Manager, set the *Firewall Forwarding URL* attribute on the *Security* panel for each array member to:

`http://127.0.0.1:443`

- Restart each Secure Global Desktop server in the array. It is recommended that you restart the primary server last.

See also *Administration Guide » Security » Using Secure Global Desktop with the HTTPS port through a firewall*.

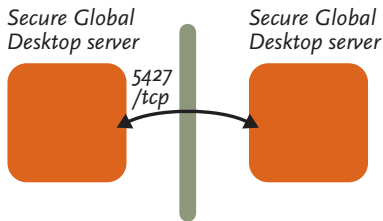


Figure 13-F: Traffic between array members uses port 5427/tcp

13.5 FIREWALLS BETWEEN ARRAY MEMBERS

There may be firewalls between array members. For example, if you have multiple offices, each containing a Secure Global Desktop server, you may restrict network traffic between them using a firewall.

Connections between array members are always to port 5427/tcp (no other ports are used for Secure Global Desktop-related traffic between array members). An array member must be able to connect to any other array member.

Port 5427/tcp is registered with IANA for use with Secure Global Desktop.

There may be firewalls between Secure Global Desktop servers and application servers. These will be firewalls within the organization, and are more likely to be configurable.

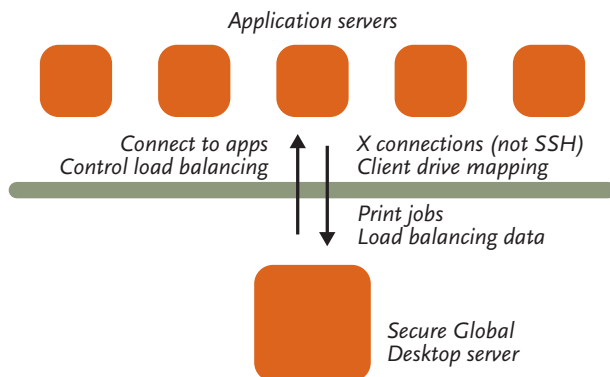


Figure 13-G: Traffic between Secure Global Desktop servers and application servers uses various ports

Which ports you need to open (and in which direction) depends on the types of application and the Secure Global Desktop functionality you're using.

Connections *from* a Secure Global Desktop server *to* an application server:

- 22/tcp For X and character applications using SSH.
- 23/tcp For Windows, X and character applications using telnet.
- 512/tcp For X applications using rexec.
- 513/tcp For X applications using rlogin.
- 514/tcp For X applications using rcmd.
- 3389/tcp For Windows applications configured to use the Windows Terminal Services protocol.
- 3579/tcp For controlling the Secure Global Desktop load balancing service running on an application server (from the primary server in the array only).
- 5999/tcp For Windows applications configured to use the Wincenter protocol with the telnet connection method.

Connections *from* an application server *to* a Secure Global Desktop server:

- 137/udp For WINS services with client drive mapping.
- 139/tcp For client drive mapping services.
- 515/tcp For print jobs.
- 3579/udp For periodic reports of load balancing information (to the primary Secure Global Desktop server only).
- 6010/tcp and above For connecting X applications to Protocol Engines, when the connection method is *not* SSH.

Ports 3579/udp and 3579/tcp are registered with IANA for use with Secure Global Desktop.

13 Firewalls and proxy servers

13.7 OTHER FIREWALLS

Other firewalls may be in place in your network infrastructure that restrict connections between Secure Global Desktop and any authentication services and directory services you might be using. To use these services through a firewall requires these open ports:

137/udp, 139/tcp	To a Windows server, for use with the NT login authority.
389/tcp	To an LDAP directory, for use with the LDAP login authority and/or Directory Services Integration.
636/tcp	To an LDAP directory over an SSL-based (LDAPS) connection, for use with the LDAP login authority and/or Directory Services Integration.
1024/udp to 65535/udp	To an RSA SecurID/ACE server, for use with the SecurID login authority.
5500/udp	From an RSA SecurID/ACE server to a Secure Global Desktop server, for use with the SecurID login authority.

For more details on these ports see *Administration Guide » Security » What ports does Secure Global Desktop use?*

13.8 LESSON SUMMARY

This lesson described how Secure Global Desktop supports proxy servers and firewalls. It explained the different types of proxy server supported, and how to deal with multiple firewalls both under your control and outside your control. The lesson described how to use firewall traversal, and how to configure your array to use different external DNS names inside and outside firewalls.

13.9 REVIEW QUESTIONS

1. What is the purpose of the firewall traversal feature?
2. What are the requirements for automatically configuring a client's proxy server settings?
3. Why does Secure Global Desktop require that HTTP or HTTPS traffic must be able to reach the Secure Global Desktop server?
4. What port numbers do Secure Global Desktop servers in an array use to communicate with one another?
5. What port numbers are used for communicating load balancing information?

13

Firewalls and proxy servers

13.10 ANSWERS TO REVIEW QUESTIONS

1. The firewall traversal feature allows full Secure Global Desktop functionality over a single port. This lets you use Secure Global Desktop in restricted environments in which only one port is open through a firewall, typically 443/tcp.
2. For automatic configuration of proxy server settings for a client:
 - The client must be a web browser. (Secure Global Desktop Clients do not support automatic configuration of proxy server settings.)
 - The autoconfig file must have either no file extension or the extension `.pac`.
 - The autoconfig file must be written in JavaScript.
 - The autoconfig file must conform to <http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html>
3. HTTP or HTTPS traffic must be able to reach the Secure Global Desktop server as both web browsers and Secure Global Desktop Clients make HTTP or HTTPS connections to the web server to request information, such as the HTML, graphics, and applets used for the browser-based webtop.
4. Secure Global Desktop servers in an array use port 5427/tcp to communicate with one another.
5. Load balancing information is communicated from application servers to the primary Secure Global Desktop server in the array on port 3579/udp.