Chapter 8

Using Intelligent Application Gateway 2007

Solutions in this chapter:

- Implementing an Intelligent Application Gateway 2007
- Configuring the Whale Communication Intelligent Application Gateway 2007
- Configuring ISA Server to Allow Communication Between the Two Servers
- Utilizing the Whale Communication Intelligent Application Gateway Tools

☑️ Summary
☑️ Solutions Fast Track
☑️ Frequently Asked Questions
Introduction

The Whale Communication Intelligent Application Gateway 2007 is used in conjunction with Microsoft Internet Security and Acceleration (ISA) 2006 Server and Microsoft Internet Information Services (IIS). Microsoft acquired Whale Communications in May 2006 and shortly afterwards added the Intelligent Application Gateway to their suite of security products. When combined with virtual private networks (VPN), secure sockets layer (SSL) connections, endpoint policies, and compliance checking, the Whale Communication Intelligent Application Gateway 2007 will allow users to securely connect to servers where Web-based applications are stored.

End users are able to securely connect to a Web portal through the Whale Communication Intelligent Application Gateway 2007. Security over the Web is paramount for companies; important data about users and the organization can be exposed when mail is sent via the Web in plain text format. Network users are able to connect to Web-based applications, such as Outlook Web Access and Lotus Notes (IBM).

In summary, the Whale Communication Intelligent Application Gateway 2007 is a component of Forefront Edge Security and Access. The Intelligent Application Gateway (IAG) allows users to connect servers through portal Web sites. When users are connected to Web-based applications using Secure Sockets layer traffic, they are less likely to encounter the vulnerabilities associated with Web sites and portals whose traffic is not encrypted. The Whale Communication Intelligent Application Gateway 2007 with ISA 2006 Server, secure endpoints, virtual private networks, and compliance checking can help companies avoid the common vulnerabilities associated with remote clients connecting to their networks.

The History of SSL VPNs

Organizations were looking to utilize the global connectivity aspects of the internet to provide access to corporate resources. It started with customers and, of course, employees traveling to do business between national or international sites, as the productivity gains were both obvious and immediate.

There were few technologies that could provide this functionality.

The first to arrive was dial-up access, which was rather costly. Dial-up is sometimes the only choice available for most rural or remote areas where broadband provision is unlikely due to low population and demand. Low access speeds mean that users have a limited remote access experience connected to the corporate servers.
Next, there was a wave of reverse proxies, publishing Web-based applications to the outside world. An example of this would be the ISA Firewall's Web Publishing feature set. This delivered value but was limited to Web-based applications. However, it did add an additional layer of defense and encryption compared to previous remote access solutions.

There followed a wave of IP security (IPsec) VPN solutions that transitioned from the normal site to site solution to an encrypted client/server VPN. Employees got complete access to the company network, as they had when sitting in front of their corporate desktops. When connected over a faster Internet connection (for example, an ISDN 128 Kbps line), the connected experience was immensely superior to dial-up modem connections. End user experiences improved again when high-speed Internet connections (broadband, cable Internet, leased lines) from 1 Mbps upwards became available from home, hotels, and conference centers across the world.

The IPsec VPN solutions had its limitations; for one, it lacked security. The other significant problem was that the IPsec VPN client required to connect to the VPN became large and difficult to roll out. This was due to its requirement for client firewalls and antivirus inspection in order to make up for the lack in security. IPsec VPNs, while widely implemented, rarely gets used for end-to-end protection of application protocols. It is mainly used today as an “all or nothing” protection for a VPN.

One of the things that SSL VPN brings to the table is taking all of these current solutions and consolidating them into one platform. SSL VPN means access for:

- Any user
- Any location
- Any application

The current wave is focused on application intelligence; this is what is needed to ensure access for any user from any location to any application stays secure without the very large IPSEC VPN client tool. This has led to the current generation of SSL VPN features that are present in every SSL gateway. All these features are implemented at both the client and gateway:

- **Client side security** Endpoint security or endpoint policies
- **Tunneling** Tunnel non-Web and Web applications
- **Pre-authentication** Authenticate before contacting corporate servers
User Portal  Made available after the user has logged on; this is where access to published applications is found

Authorization  Allow and Deny access to the portal or the applications hosted in the SSL VPN portal

Application Layer Inspection  Some form of application layer inspection needs to be provided in order to qualify as an enterprise grade SSL VPN gateway.

Implementing an Intelligent Application Gateway 2007

History shows that if you want to implement a secure and stable firewall, remote access, or an enterprise resource planning (ERP) product, such a product must be the only hosted solution on an extremely security-hardened appliance.

With this in mind, Microsoft has partnered with original equipment manufacturers (OEMs) to bring Microsoft’s Intelligent Application Gateway (IAG) and Microsoft Internet Security and Acceleration (ISA) server-based security appliances to the market. These two solutions combined bring IAG 2007 and the best of ISA 2006 Server, with a comprehensive-hardened configuration of Microsoft Windows Server 2003, configured on optimized hardware so that the appliance is ready to be rolled out straight from the box. IAG 2007 cannot be installed; it is only supplied preinstalled in an appliance form.

For client access, IAG has two types of license: the client access licenses (CAL) and the external connector (EC) license. With the EC license, there is no need to buy individual IAG 2007 CALs. An EC license is not mandatory; it’s a license that can be used by business partners or customers instead of using CALs. License types are available through a network of channel partners, resellers, and Microsoft’s volume licensing program.

The implementation stage and the ability of IAG 2007 to be adapted to a multitude of environments within an enterprise makes for easy deployment, even when expanding existing SSL VPN implementations within the organization. The ease of deployment goes hand in hand with the ease of implementing popular enterprise applications, hence the current focus on Application Intelligence in SSL VPNs.

Unlike other SSL VPNs where administrators have to do complicated technical configuration in order to get popular internal applications published onto a Web portal, the IAG 2007 administrator simply selects from a list of “out of the box” applications provided by Microsoft. IAG 2007 then performs most of the setup automatically. The hard work has been done by Microsoft; they have put together all the popular applications available and compiled a list of security considerations linked to each
application. This is made available as automatic rule sets within IAG 2007 and ISA 2006. IAG 2007 then has the capacity to be manually changed to comply with nonstandard back-office systems and policies. This means that security can be tweaked to match complex security policies with organizations.

The major gain derived from implementing an SSL VPN is enabling access from computers which are not under company control. Taking this into consideration, the organization will need to implement endpoint policies to control access to corporate servers from unmanaged devices. Endpoint policies need to be implemented to state which conditions must be met by managed or unmanaged devices to gain access to the organization’s SSL VPN and or applications made available on the Web portal. Until now, SSL VPNs did not have the ability to fully enforce such policies. These policies can be anything from a personal firewall that needs to be installed and up-to-date on end-user computers to a specific operating system that is not allowed on the SSL VPN.

ISA Server runs on the IAG server. The ISA configuration is maintained by IAG. Figure 8.1 shows a typical IAG SSL VPN.

**Figure 8.1 A Typical IAG SSL VPN**

---

**Configuring the Whale Intelligent Communication Application Gateway 2007**

Configuring IAG 2007 to be a working SSL VPN out of the box, is a very easy process to follow, not only for the already experienced SSL VPN administrator, but also by an
SSL VPN administrator new to the world of VPNs. Once such a working gateway has been configured it can be tweaked in such a way as to become a very powerful and secure globally-used and standardized solution for an organization. Customizing IAG 2007 to fit with nonstandard organization-wide policies has never been easier, and enabling users to utilize well known internal applications from managed or unmanaged devices has never been as simple as with the IAG 2007 and ISA 2006 Server combination.

In this section we will be looking at not only running an out-of-the-box solution but also fully customizing a standard IAG 2007 solution. This will include creating a portal trunk, which will provide access to multiple applications via a single Web portal, and all of the steps necessary to complete and activate the portal in order to use nonstandard organization-wide policies on a secure SSL VPN.

Configuration Page

The IAG Configuration page is where most of the SSL VPN creation and configuration takes place. This is also where application access and endpoint policies are configured. From this configuration window, portals can be created, applications added, and necessary security changes made (see Figure 8.2).

**Figure 8.2 Intelligent Application Gateway Configuration Screen**
This page and all configuration changes made on this page are secured by a passphrase, which is set up during the initial IAG configuration procedures.

**Note**

For more information on passphrase and passphrase encryption, refer to the section “Passphrase” later in this chapter.

From here, additional changes can be made. For example, you can create a highly available IAG portal when expanding an existing SSL VPN implementation and make the necessary advanced trunk configuration changes when security policies need to be altered. Examples of changes to security policies include changing the Web server certificate, making authentication changes, changing session settings, tweaking URL inspection, and customizing an application.

From here, the portal backup can also be run, procedures restored, and IAG user access completely monitored.

**Application Access Portal**

End users will connect to a privately developed and owned, closed-system architecture, a Web-based application access portal to a variety of centralized resources, ranging from traditional client/server applications to Web and intranet applications by using the following URL based on Figure 8.3: https://syngress.local.

All transmissions between IAG and the local machine are encrypted using SSL (secure socket layer) technology, while site authenticity is assured through built-in digital certificate support. End users will only be able to see and log in to this page based on endpoint policies defined on the Web portal or application. The port defined here is the port number of the external Web site.

**Figure 8.3 Application Access Portal**

![Application Access Portal](image.png)
External Web Site

Figure 8.4 shows the external Web site where the open port and the IP address are configured and changed to connect to the Web portal. This is typically the external network cards IP address of IAG appliance. This IP address is configured during the portal trunk configuration.

**Figure 8.4 External Website**

![External Website](image)

A list of IP addresses and port numbers can be created by using the Service Policy Manager to control the IP addresses and port numbers that are used to access the internal network. This step is needed to enforce the selection of predefined IP addresses and port numbers during trunk configuration.

**Note**

For details of the Intelligent Application Gateway Service Policy Manager, refer to the section at the end of this chapter titled “Intelligent Application Gateway Service Policy Manager.”

Initial Internal Application

Figure 8.5 shows the initial internal application section on the configuration page. This is where the internal application to be displayed on the Web portal can be specified after the user has successfully logged on. The default setting is “Web Portal,” which will display a list of available applications published by the organization.

**Figure 8.5 Initial Internal Application**

![Initial Internal Application](image)
However, any of the applications published can be selected to be the initial internal application; when choosing anything other than the default, the Use Toolbar tick box will become available. In the scenario where the administrator selects OWA to be the initial internal application and to the Use Toolbar option, the end user would have the following toolbar when logged on to the Web portal (see Figure 8.6).

**Figure 8.6 Web Portal**

The result would be that when an end user logs on to the Web portal, the first thing to be loaded will be the end user’s OWA. To continue the user can choose from any of the available published applications on the toolbar.

This will be the only way that the user will be able to navigate around the Web portal. The “Whale Portal” will no longer be available. In this scenario, when clicking on the IAG homepage icon on the toolbar, OWA will open as it is in the initial internal application.

**Security and Networking**

Figure 8.7 shows the Security and Networking section on the configuration page, where advanced trunk configuration and high availability can be modified. More high
availability servers can be added to the configuration by navigating to the Admin High
availability servers menu in the menu bar of the IAG Configuration page.

The advanced trunk configuration section allows the SSL VPN administrator to
configure options otherwise left unconfigured by default. These options include:

- **Server Certificate** Certificate issued to the external site.
- **Website Logging** Enable detailed Web portal logging.
- **Authenticate User on Session Login** What type of authentication used.
- **Logoff Scheme** Logoff URL, message, and session termination.
- **Session Configuration** Session limits and attachment wiper.
- **Endpoint Policies** Web portal endpoint policies.
- **Application Customization** Allows IAG to customize published applications.
- **Application Access Portal** The intelligent application portal.
- **URL Inspection** See host address translation (HAT).

**Figure 8.7 Security and Networking**

![Security & Networking Configuration](image)

The major technical challenge SSL VPN administrators face regarding providing
access to internal applications across the Internet is within the applications internal
references. IAG 2007’s host address translation (HAT) engine encrypts and translates
any number of internal host names to a single external host name. End users will
never have the ability to launch attacks based on what they see in the Web portal.
In other words, http://internalservername:80/application will become https://external.
hostname/whalecom/whalecom0/application.

IAG 2007 delivers data over a standard browser for end users to securely access sensitive
information by overlaying industry-standard 128-bit encryption SSL. This prevents
hackers intercepting and reading data. Only one-time authentication or one certificate
is necessary, despite the user accessing a number of different published applications
and server resources.
To prevent logon credentials or any other information from being cached on managed or unmanaged devices, IAG 2007 utilizes patent-pending Secure Logoff technology. This proprietary and innovative mechanism eliminates the possibility of malicious users reinstating user sessions.

Attachment Wiper

Upon completion of the end user SSL VPN session, the attachment wiper will remove all traces left on the unmanaged or managed device that was created during the session. This is triggered by the following:

- When a user logs off from the session.
- The computer browser is closed down.
- The computer browser experiences a crash.
- The managed or unmanaged device is shut down.
- The session logoff threshold passes.

Upon any of the above occurrences the attachment wiper removes the following:

- AutoComplete entries in the computer browser address bar and form field contents.
- Attachment temporary files.
- User credentials.
- Computer browser cookies downloaded during the user session.
- Computer browser history generated during the user session.
- Any temporary downloaded or created files generated during the user session.
- All computer browser cache entries.

Endpoint policies can be created to administer the attachment wiper. The attachment wiper will remove the listed information above, created when an end user’s SSL VPN session is active.

The hard drive clusters on the unmanaged or managed device on which the end user has stored files will be overwritten with other data by the attachment wiper seven times to make it technically impossible to undelete or reinstate those files. Thus, the attachment wiper conforms to the DoD-acceptable way of sanitizing magnetic
Applications
Publishing internal applications is in the center of the new application intelligence wave of SSL VPNs. Microsoft’s IAG 2007, together with ISA 2006, has made publishing an internal application one of the easiest processes.

**Exercise:** Adding a published application to the Web portal.

1. In the Application section in the IAG portal click Add, which will bring up the Add Application Wizard (Figure 8.8), giving you the choice of what kind of application you want to publish.

**Figure 8.8 Add Application**

![Add Application Wizard](image)

2. In this example we are going to add Microsoft Outlook Web Access 2007 Web Application. Click Next. In the wizard (Figure 8.9), name the application “OWA 2007”. You can specify whether all users are authorized and you can set endpoint policies. Click Next.
3. Add the name of the internal exchange server, choose port numbers (Figure 8.10).

**Figure 8.9 Application Setup**

![Add Application Wizard](image1)

**Figure 8.10 Web Servers**

![Add Application Wizard](image2)
4. Choose the Authentication Servers (Figure 8.11).

**Figure 8.11 Authentication**

![Authentication Wizard](image)

5. Add the link to the portal and toolbar and click **Finish** (see Figure 8.12).

**Figure 8.12 Portal Link**

![Portal Link](image)
Figure 8.13 shows a typical list of Web portal published applications. From this window the SSL VPN administrator can add or remove applications. This window is also where the sort order for applications listed on the Web portal can be chosen.

**Figure 8.13 List of Published Applications**

Limiting Applications on Subnets

Figure 8.14 shows where the SSL VPN administrator can restrict any of the applications made available on the SSL VPN Web portal so that only servers within the defined subnets are enabled for use from the Web portal. Once the trunk is activated and an end user requests a URL from the Web portal, the filter will first check the URL against the application list. If the application is listed, then the filter will check on the URL against the subnet list. Only if the URL passes both checks will the application be enabled to the user.

**Figure 8.14 Subnets**

**NOTE**

For each application added, make sure that the application is listed in the IAGs DNS or HOSTS file.
Subnets are configured in the main window of the Configuration program, in the “Applications” area.

Creating a Trunk

When a new trunk gets created, the Configuration program activates the Create New Trunk Wizard (see Figure 8.15). This enables the administrator quick auto-complete of the initial trunk setup, external Web site, authentication, application customization, and URL inspection rules. A trunk can be made under the HTTP and the HTTPS services.

Tip

It will be useful to go through the IAG Service Policy Manager a. It is possible to preconfigure a list of IP addresses and port numbers, which you can use to assign IP addresses and port numbers to the services when creating and editing trunks.

Figure 8.15 Create New Trunk Wizard
Basic Trunk

Basic trunks enable the establishment of a one-to-one connection, where one IP address routes to a single generic Web application. This type of trunk will be used in a scenario where the organization has a single Web application, which will be of benefit to be published to a Web portal.

During the setup process, select the public host name, external IP address of the portal, and the ports used. Next, setup authentication by choosing the appropriate certificate for this application and pointing to the actual application server with an optional path to the application. Then set up optional application authentication and, lastly, the endpoint policies.

Portal Trunk

An HTTP or HTTPS trunk has incoming and outgoing channels, allowing for bidirectional data flow. Unlike the other trunks a portal trunk is a one-to-many connection, where the same IP address is used to access multiple applications. It can be used to enable Web and non-Web applications, generic and out-of-the-box applications.

To create a portal trunk:

1. In IAG, right-click HTTPS Connections and choose New Trunk. From the options, choose Portal Trunk, and click Next.
2. Give the trunk a name and enter the Public Hostname/IP address of the Web portal. Add the IP address of the external Web site and choose which port you want to use for HTTP and HTTPS.
3. Select Servers for Session Authentication, click Add, and set up the needed type of authentication. During this process, select whether end users will need to authenticate only once or for each selected server.
4. Configure the Server Certificate by choosing the certificate that will secure the SSL Web portal. For the certificate to show in this window, it must be issued to the IAG server. The certificate manager can be launched for the local computer from this window in order to do local certificate management.
5. Session Access Policy controls access to the trunk, depending on endpoint policies. Privileged Endpoint Policy defines a policy for endpoints that enjoy session privileges. The necessary policies can be edited from this window. Click Finish.
Webmail Trunk

Webmail trunks are dedicated trunks for a single Webmail application, and are automatically created with authentication, application customization, and URL inspection rules that are optimized for the specific Webmail application being run on this trunk.

When creating Webmail trunks, it is recommended that the HTTPS Connections service be used.

Redirect HTTP to HTTPS Truck

It is very easy for an end user to use HTTP instead of HTTPS by accident. The SSL VPN administrator has to make sure that HTTP requests made to the Web portal are redirected to HTTPS by the organization and not by a third party with malicious intentions. When an HTTPS request is made to the Web portal, the request will be handled by the HTTPS trunk. If the requirement is there to redirect HTTP requests to the HTTPS trunk, it can be done by creating an additional redirect trunk.

The redirect HTTP to HTTPS Trunk option in Figure 8.16 will only become available if you select to create a new trunk by right-clicking on HTTP connections.

### Note

A trunk can be deleted in the Configuration program by selecting the trunk in the list pane, and then selecting DELETE from the right-click menu.

Activating an IAG Configuration

Configuration changes on the IAG need to be implemented in various scenarios. Starting with when IAG is being set up in the initial stages of SSL VPN rollout. In the scenario where large organizational security policy changes or a small configuration change to the IAG configuration needs to be implemented, the configuration needs to be activated.

Saving and activating an IAG configuration enable the changes in the Web portal. This step also provides you with the option to back up the configuration and to apply the changes to external configuration settings (see Figure 8.16).
Backing up the IAG configuration can be done from this window so that configuration settings are backed up and changes are activated in one step. During a backup procedure, the IAG will make use of the Windows makeab.exe utility to archive the necessary files and Registry values in a .cab file. By default, the backup is created under the IAG installation path: …\whale-Com\e-Gap\Backup.

The name of the backup file that is created in the defined backup folder is whlbackup.<host_name>.cab, where host_name is the name of the IAG.

Restore from Backup in the IAG Configuration program from uses the Windows extract.exe utility to restore the files.

To restore the configuration in the configuration program:

1. From the Admin menu, in the Configuration program, click Restore from Backup.
2. Then activate the Configuration, to make the restore configuration. Then activate again.

Once the configuration is activated, the following message is displayed: IAG configuration activated successfully.
The trunk is now operational. All users who authenticate to the Web portal will be able to access the applications published through it.

**Passphrase**

After the initial rollout of the IAG, the first time the Configuration program or the Service Policy Manager is accessed, it is required to create an encryption key and passphrase for the IAG. Because both IAG applications are served by encryption key and passphrase, so this action is only required once. The same passphrase is used when subsequent access is made to either of these applications.

The encryption key is used to encrypt the configuration data. In high IAG availability arrays, all of the IAG servers need to be configured with and identical encryption key. Identical keys are needed in order to import and export configuration files between the IAG servers and to import and export URL inspection and File Access rule sets.

---

**TIP**

When using the Configuration program, the encryption passphrase entered is valid for 10 minutes. That is, during the 10 minutes following an operation that requires access to the configuration files, the files can be accessed again without having to reenter the passphrase.

---

**NOTE**

If different keys have already been defined on different IAG servers and they need to be unified, these steps can be taken:

- To export the encryption keys, run the following utility in a command line, on one of the IAG servers ...\whale-com\e-gap\common\bin\exportkeys.exe.
- To import the encryption keys to the other IAG servers, run the following utility in a command line, on each of the servers ...\whale-com\e-gap\common\bin\importkeys.exe.

---

**Internet Information Services Manager**

In addition to the first portal trunk created, the Create New Trunk Wizard automatically creates an external Web site on the Internet Information Services (IIS). IAG creates and maintains the configuration of the Web portal site.
In some circumstances you might need to restart the IIS Web Service on the IAG server, as described in the following steps:

1. Click **Start | All Programs | Administrator | IIS Manager**.
2. Select the **Local** server. Right-click and choose **All Tasks | Restart IIS**.
3. From the available choices, start, stop or restart IIS.

The port numbers IAG use to communicate with the IIS default Web site is port 6001 for HTTP and port 6002 for HTTPS (see Figure 8.17). If an application published by IAG is using one or both of these ports, the port number can be changed, as described below.

- From the Admin menu in the Configuration program, click **Advanced Configuration**.

**Figure 8.17 Advanced Configuration**

![Advanced Configuration](image)

1. In the Default Web Site Ports area, replace the default HTTP or HTTPS port numbers, as required, and click **OK**.
2. Activate the configuration.

**Viewing Remote Computer Certificate**

Once an end user is connected to the newly created Web portal, making sure the session is secure before logging on is one of the most important steps because the end user wants assurance that his logon username and password are encrypted.
First, the SSL VPN administrator must keep in mind is that the HTTPS Web portal needs a valid and secure enough certificate attached to it. The way to do this is to make sure the new IAG gateway has a new certificate attached to it and that the certificate is valid for a long period. It is suggested to request a certificate be issued for a two-year period or longer. Second, the administrator should make provision for users accidentally connecting to the Web portal with HTTP instead of HTTPS. The way to do this is to create a Redirect HTTP to HTTPS Trunk in the IAG.

Depending on the end user’s Internet browser, the certificate will be accessible when the end user browses to the IAG Web portal. A padlock will be displayed and double clicking the padlock will display the remote computer’s certificate. By doing this the end user can see the following options:

- Issued to: this will display the public host name to which the certificate is issued.
- Issued by: the certificate authority (CA).
- Valid from: The valid from and valid to date of the certificate.

Configuring ISA Server to Allow Communication Between the Two Servers

The IAG 2007 actually has the 2006 ISA Firewall installed on it. The ISA configuration is maintained by IAG, making it a completely appropriate edge device. The ISA firewall has never been compromised and has no security issues; because of this, it makes sense to design an organization’s SSL VPN on an IAG server.

IAG Firewall Rules (13)

With the IAG and ISA server so closely joined together, Microsoft has made creating a portal with published applications and the related firewall changes in ISA server into one process. When the IAG configuration is changed and the configuration activated, IAG will update the related firewall rules in ISA.

The first thirteen rules allowed in ISA were created during the installation of IAG. Figure 8.13 shows the list of firewall rules created in ISA server by the IAG after the configuration was activated. For example, rule 11 shows protocol UDP on port 53 is allowed to enter the firewall and go through to an internal server for all users.
Portal Trunk Configuration Rules (2)

The portal trunk configuration “allow” rules were created when the portal trunk was activated. After portal trunk activation, testing can start and the portal Web page can be used.

The second of the two allow rules is the Whale::Auth#001 rule (see Figure 8.18). This is the rule that allows connection to the Domain Controller, which in turn allows the Active Directory to authenticate the session. This rule is also the rule that will be used for whatever authentication setup during the configuration of the portal.

Figure 8.18 ISA Server

Utilizing the Whale Communication Intelligent Application Gateway Tools

One of the most important jobs the SSL VPN administrator is to make sure that the IAG gateway continues to run in good health even if it experiences unexpected high
volume of requests. In a support environment around the IAG, it is very helpful to have a full range of tools to aid the administrator in resolving either potential disastrous events or small end user problems.

With IAG it has been made even easier to support such a VPN solution. It is recommended that the IAG configuration and security policies be documented; this will aid troubleshooting problems which might occur with IAG or an end user session.

**Whale Communication Intelligent Application Gateway 2007 Web Portal**

A Web portal provides a service to end users. These services are made available depending on the Web portal needs of the organization. This opens up more possibilities of problems that can arise from the use of the Web portal. These services could be a list of defined applications made available to employees on the road, and even customers. The SSL VPN administrator could use the Web portal in order to resolve a number of problems.

The end user experience on the IAG Web portal can be improved. Some tools are made available to the end user to utilize during an active session on the Web portal. The main goal of these tools is to eliminate a large portion of support calls that can potentially be made to a support desk.

**Defined Applications**

Defined applications are the applications the SSL VPN administrator published after creating the portal trunk. This list of applications is available in the Web portal to the end user. The list is also available in the toolbar on the Web portal.

Depending on endpoint policies set up and based on the managed or unmanaged device connecting to the Web portal will the end users see a list of defined applications. The SSL VPN administrator has the ability to make an application portal link on noncomplying devices in the endpoint policy show up grayed or invisible. This can be done on the General tab of the IAG Configuration page.

**Credentials Management**

Working in an environment where there are potentially hundreds or even thousands of end users who not only work in the office or at home, but also work on the road or remote offices, user password management issues will arise. IAG Portal has added a feature to the Web portal so the user can experience a one-stop shop for credential management.

The SSL VPN administrator can enable the “Credentials Management” option in the Portals Advanced Trunk area of the Authentication tab.
When this option is activated (applicable for portal trunks only), a “Credentials Management” button is automatically added to the Web portal homepage, enabling end users to initiate the following options any time during a session:

- **Add authentication credentials** This option is accumulative. If the end user enters two sets of authentication credentials, then both sets are applicable to that session. Each set is then used for the relevant applications.

- **Change their password** This option is applicable only when the option “Enable Users to change their passwords” is activated on the Authentication tab during the portal configuration.

**Note**

Credential Management can only be accessed if the remote user has successfully logged into a Web portal session. Only then can the user make changes to passwords or add authentication credentials.

**System Information**

The system information window can be accessed from the Web portal by the end user. The information on the page will give the end user a better idea of what has been installed on the managed or unmanaged device (see Figure 8.19).

If the end user is experiencing difficulty doing something in particular on the Web portal, the system information will aid the SSL VPN administrator when supporting the end user and the certified endpoint status determination.

End users can check whether the Whale client components are installed on their system. They can also:

- **Uninstall Whale client components.**

- **Restore component defaults** End users can restore the Whale client components settings on their computer to the default values.

- **Delete the user-defined trusted sites list** Once users add a site or a number of sites to the list, they can remove them from the list via the System Information window.
Activity

The portal activity window will be available in a portal trunk and a Webmail trunk. To open the portal activity window double click the portal activity icon in the windows system tray (to the right of the taskbar).

- **Connections area displays** The active channel and the connections. Double clicking the connection will show the number of bytes sent.

- **Application area displays** The list of application launched.

The end user can also disconnect a session from the Activity window.

Email System Administrator

Email System Administrator is another tool available on the IAG Web portal. This will open a new email message with the Administrators email address predefined in the “TO” field.
Strategically placed on the Web portal, end users can easily come into contact with the system administrator in order to raise a help desk call or even to suggest changes.

**Whale Communication**

**Intelligent Application Gateway Editor**

If wanting to encrypt or decrypt any of the IAG files that are encrypted during day-to-day operation, the editor is the interface to use (see Figure 8.20). It enables easy editing, sorting, and conversion of any text file, including encrypted files and Base 64–encoded text. The editor can be opened by navigating to **Start | All Programs | Whale Communications IAG | Additional Tools | Editor.**

**Figure 8.20 Editor**

Using the Editor program, it is possible to:

- Save and encrypt files.
- Open multiple files simultaneously.
- Decrypt and edit encrypted files.
- Open and edit text (ASCII) files.
Use the sort and find to locate the required text.

Convert a text selection to and from Base 64 format.

Once the file is open, the title bar indicates whether the file is encrypted or not.

Whale Communication Intelligent Application Gateway Service Policy Manager

A list of IP addresses and port numbers can be created by using the Service Policy Manager. This is done to preconfigure the IP addresses and port numbers for HTTP and HTTPS connection services, which are used to access the internal network. This is needed to enforce the selection of preconfigured IP address and port number during trunk configuration.

The Service Policy Manager can be opened by navigating to Start | All Programs | Whale Communications IAG | Additional Tools | Service Policy Manager (see Figure 8.21).

Figure 8.21 Service Policy Manager
Whale Communication
Intelligent Application Web Monitor

The Web Monitor is a complete solution for the SSL VPN administrator to monitor all user session events (see Figure 8.22). It is integrated within the system as a SSL VPN–supported application with its own Intelligent Application Optimizer. It allows the administrator to zoom into a user’s Web portal session in real-time. Users with application access problems will be easily identified and solved with IAG working at the application level. The Web Monitor is essential in the administrators day-to-day support functionalities. The Web Monitor also gives the administrator event filtering and analyzing capabilities.

The Web Monitor can be opened by navigating to Start | All Programs | Whale Communications IAG | Additional Tools | Web Monitor.

If an IAG high availability array is deployed in an organization, one can make use of the Web Monitor to monitor all the IAG servers that are part of the array.

Redirect trunks are not monitored by the Web Monitor.

Figure 8.22 Web Monitor
Creating and Managing Intelligent Application Gateway Endpoint Policies

Microsoft’s Intelligent Application Gateway 2007 (IAG) is a hardware appliance that integrates technology purchased from Whale Communications in the summer of 2006 and the vendor’s own Internet Security and Acceleration (ISA) Server.

IAG 2007 is ideal for IT managers, network administrators, and information security professionals who are concerned about the security, performance, manageability, and cost of network operations.

IAG 2007 combines an SSLVPN with endpoint security checks and firewall features, enabling the creation of policy-based remote access controls to a network and its individual applications. This “access portal” features three levels of policy-based traffic filtering at both the packet and application layers. End users access the platform through their Web browsers with communications being protected via SSL encryption; and policies can be defined specifying which users and/or machines are enabled access to which network resources.

Access to the IAG appliance from remote locations is accomplished with any Web browser. Microsoft lists multiple browsers as compatible; however, Internet Explorer has components that enable specific features of the gateway that are available only as ActiveX controls. Therefore, full functionality requires a Windows and Internet Explorer based endpoint.

The IAG 2007 provides a means to create an access portal to corporate network applications, accessible by a Web browser, which allows end users to authenticate their credentials and access only those applications and features that their administrators’ defined policies allow. IAG 2007 supports an unlimited number of users, and up to 64 IAG nodes can be combined in a high-availability configuration, thus meeting corporate needs.

Access to corporate applications is assisted through the use of specialized “application optimizers,” which are available from several Microsoft and third-party software offerings, including Microsoft Exchange server and Microsoft SharePoint portal server. These application optimizers consist of integrated software modules with preconfigured settings designed to allow access to the target applications through the IAG portal. Features provided by the optimizers to the target applications include single-sign-on support with
the ability to apply certain granular rights assignments per user policy, and support for “attachment wiper,” which removes and scrubs temporary session data from the client, including browser history files and pages, auto complete form contents, temp files, cookies, history, browser closure, and system shutdowns such as logoff and browser failure. Last but not least, the optimizers also even blocking file uploads if an approved virus scanner is not present on the endpoint machine. For example, the systems administrator could define a policy that if a remote user does not have the latest version of the corporate anti-virus solution, the user(s) will not be allowed to upload any attachment to their mailboxes.

IAG Server simply eliminates the risk of network attacks and operating system vulnerabilities as it only provides a means to access specific applications (or some of the features only) to approved users from approved machines.

Another notable feature includes the capability to have individual client tools that can be downloaded to the endpoint, enabling additional features of the portal. (Again, many of these features require a Windows-based endpoint and browser.)

Some of these features include:

- **End Point Detection** The ability to examine the endpoint’s anti-virus checking capabilities. End point detection can work in combination with policy-based access; that is, a user can be allowed or disallowed to perform certain functions depending on their endpoint posture.

- **SSL Wrapper** The ability to transport certain network protocols (terminal services, RPC, terminal emulation) over an SSL connection via port-forwarding or socket-forwarding models.

- **Network Connector** The ability to enable full networking connectivity from the client via a bidirectional VPN tunnel. The network connector provides remote users with a local IP address as if they were directly connected to the corporate network.

Together these technologies provide mobile and remote workers with easy and flexible secure access from a broad range of devices and locations, including kiosks, PCs, and mobile devices anywhere the road warrior or remote user is based.
Summary

In this chapter, we reviewed the history and basics of the Intelligent Application Gateway. Understanding the history of SSL VPNS will help you get closer to the goals we defined at the beginning of this book. The design and planning stages are just as important as planning any other business-critical solution in the organization. Configuring IAG to be a secure application-sharing and robust SSL VPN tool will prove priceless for any sized organization.

Publishing business-critical applications has never been easier, and has never been as comprehensive as with Microsoft’s combined IAG and ISA Servers. SSL VPNS not only brings the organization closer to a standardized way of accessing applications "on the road", but also moves the organization forward. Building a robust organizational SSL VPN has numerous benefits to employees and even customers.

We looked at creating different types of trunks for different scenarios, all the rules that apply to activating a trunk, and we discussed the importance of backups. The Web portal has all the relevant tools needed by the end user, and is a complete experience.

From a security perspective, it is important to remember that IAG with the built-in ISA Server is a complete, secure solution in one appliance on a hardened operating system. The importance Microsoft has put on security combined with the ease of creating firewall rules restricting access to only published applications and using endpoint policies together makes IAG a proven solution.

Solutions Fast Track

Implementing an Intelligent Application Gateway 2007

- For client access, IAG has two types of license: the client access license (CAL) and the external connector (EC) license.
- Application intelligence.
- Endpoint policies.

Configuring the Whale Communication Intelligent Application Gateway 2007

- Configuration screen.
- Publishing an application.
Creating a trunk.
Activating configuration.

Configuring ISA Server to Allow Communication between the Two Servers
- Firewall rules.
- Portal trunk firewall rules.

Utilizing the Whale Communication Intelligent Application Gateway Tools
- Credential management.
- System information.

Creating and Managing Intelligent Application Gateway Endpoint Policies
- IAG 2007 combines an SSL VPN with endpoint security checks and firewall features, enabling the creation of policy-based remote access controls to a network and its individual applications.
- Access to the IAG appliance from remote locations is accomplished with any Web browser.
- IAG 2007 supports an unlimited number of users, and up to 64 IAG nodes can be combined in a high-availability configuration.
Frequently Asked Questions

Q: Is it possible to limit the Web portal to a certain network segment for testing purposes?
A: By default all subnets are open to the published applications. However, the portal can be set up to limit the published applications to a set of subnets. It can be beneficial to implement this, as isolating certain applications during testing periods is necessary in order to make sure all endpoint policies are configured correctly.

Q: A few end users have reported that some published applications are grayed out on the Web portal and they cannot click to use the application.
A: Endpoint policies have been designed to govern which rules on managed or unmanaged devices the end user must adhere to. The “access” endpoint policy has two options for noncomplying clients: grayed or invisible. This can be achieved by accessing the published applications property page.

Q: Why should I choose IAG Server instead of an ISA server only?
A: On top of all the advantages ISA server will bring to the organization, IAG has the added advantage of granular policy control, advance security and manageability control, access from unmanaged PCs or mobile devices on unknown networks, and strong endpoint security.