# The awayWEB Virtual VPN Architecture Overview

Cris Bailiff, CTO /dev/secure
c.bailiff@awayweb.com
`http://www.awayweb.com`

21st January 2002

Satisfying the user demand for remote access to corporate information is a continual headache for IT managers. With the wide availability of ISP connectivity and services organisations wishing to move forward from the traditional legacy approach of dialup communications can leverage Internet based technology standardised on TCP/IP solutions. Most organisations now view Virtual Private Network (VPN) technology as the preferred solution to utilise this low cost, widely available infrastructure.

VPNs allow computer communications across these open, public, network infrastructures, using reliable, and proven encryption technologies. This ensures that all communications across these public networks remain private and confidential.

Whilst the principles of VPN solutions are widely understood, the reality is that designing, procuring, implementing and deploying a secure, robust VPN based solution can be a complex, slow and expensive process. Conventional VPN software must be deployed and maintained on every client machine. Corporate firewalls and other infrastructure may be incompatible with the installed system. The results may not realise the promised return on invested time and capital.

Just like a traditional VPN the awayWEB system offers secure remote access over the Internet, but without the problems of deploying client software and then making the VPN operate within the existing infrastructure. The awayWEB approach is to provide secured access to internal resources by leveraging the power of already installed commodity infrastructure - the standard web browser.

## 1 awayWEB: The Virtual VPN

The majority of corporate computer resources are already web-enabled, either natively or through web-access gateways. The awayWEB system combines web-based access with strong authentication and security to provide a highly secure infrastructure that enables secure remote access to corporate resources through the corporate firewall from any location on almost any platform.

### 1.1 The awayWEB gateway: A Firewall built for the Web

The nature of the network protocols used in web-based applications makes traditional firewall technology largely ineffective in controlling and securing access to corporate applications. Firewalls offer protection from many forms of intrusion and attack but firewalls have no real understanding of: who the users are, how they are authenticated, what privileges they have, what web applications they can access or what access constitutes a violation of policy.

To address these issues some firewall devices contain proxies, intelligent inspection, or intrusion detection systems. These mechanisms provide basic access control once users have been *authenticated* to the firewall. Unfortunately, once standard web encryption and security protocols are implemented, such as SSL/https, these mechanisms are unable to monitor or control access to web applications.

The awayWEB system provides a solution to these complex issues:

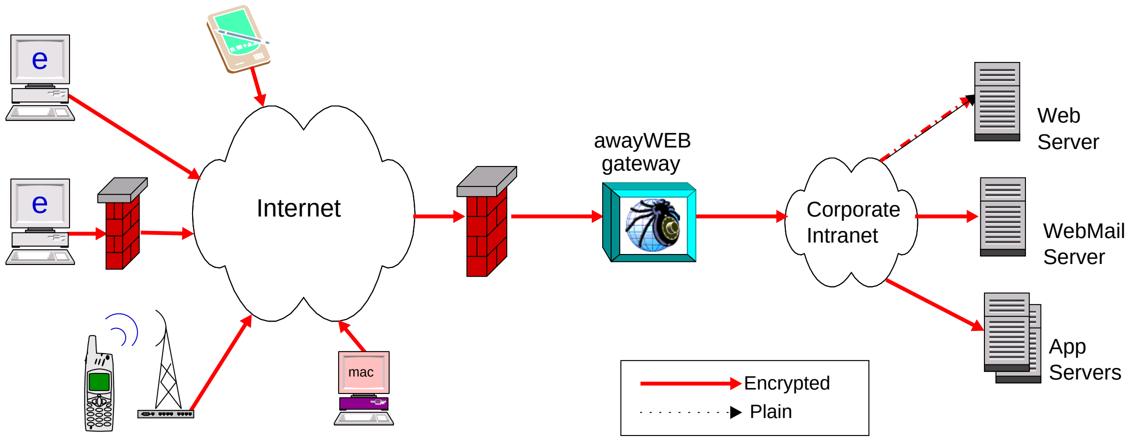


Figure 1: All intranet access must pass through the awayWEB system

- The awayWEB system operates as a centralised access control and security server, through which all remote access to intranet applications must pass. (Figure 1)
- The awayWEB system has a full understanding of the http protocol used for web applications and can make security decisions based on the users' privileges and the organisations security policy
- The awayWEB system appears on the Internet as a standard SSL enabled web server. By entering a URL or accessing a bookmark, remote users contact the gateway as they would any other web site.
- Each user must log in to the awayWEB system and then access intranet services according to the security policy defined by the organisation
- All requests passing into the awayWEB system from the Internet are decrypted by the gateway for inspection and authorisation. All information passing back to the remote user is encrypted before leaving the gateway.
- The awayWEB system translates all incoming requests and outgoing web pages so that there is never any requirement to make an internal server directly accessible to the Internet - the awayWEB system is the only directly connected system.

# 2 VPN Limits: In Detail

## 2.1 Client Software: Managing Clients

Most VPN systems require software to be installed on client devices to support strong encryption and VPN protocols. Even when some form of VPN software is included in an operating system, such as Microsoft's PPTP, it must be correctly configured with address information, encryption keys and other critical settings.

The dependence on extra installed VPN software leads to a number of issues:

- Is the VPN software compatible with the version of the operating system being used?
- Is the software compatible with the existing network configuration?
- How often must the software be updated with new configuration information?
- How is software or configuration to be updated?
- Is the operating system supported? (Maybe your partners use Macintosh or Unix?)
- Is the VPN compatible with other VPN software which may be already installed?
- Is the configuration compatible with the partner network?
- Who is responsible for maintaining and supporting the system where the software is installed?

These issues can be addressed (with some effort) for a single organisation which has control of all the infrastructure involved. Unfortunately most remote access systems also cover business partners, suppliers, vendor support and often customers. In these scenario the same issues can be much more difficult to address.

Availability of VPN client software also faces additional demands arising constantly from new network capable devices:

- PDA's and Pocket PC's
- WAP enabled cellular phones

- Internet enabled appliances, such as Web-TV and ’Smart Phones’.

Even when standard PC/Windows systems are available, it may be impossible to install or properly configure VPN software in other environments such as:

- Internet Cafés
- Airport Lounges
- Hotel Business Lounges and In-Room PC’s

## 2.2 Firewalls: VPN Configuration and Control Issues

When VPN software is properly installed and configured, its use from an unrestricted Internet access point, such as a dialup ISP account, is normally efficient and straightforward. In this situation VPN software should function ’as advertised’ and offer the user private and secure remote network access.

However, the real world experience may be different. Users are often subject to Internet access control and filtering arrangements. A remote user who is connected to a partner or suppliers company network, or even one who is using a hotel LAN or some cable access services, must access the Internet through a third party firewall security system. Most third party firewall systems will reject any traffic they do not recognise. VPN traffic appears to firewalls as a special class of network traffic. The firewalls cannot see ’inside’ the connection due to the encryption component of the VPN. The inability of the firewalls to inspect the encrypted connection means that it is against the security policy of the organisation to ’allow’ this traffic to pass. This would be equivalent to opening an un-inspected route into the network which would allow data to go in or out without being checked against the security policy. As a result most firewalls will normally not allow the connections to proceed. (Figure 2)

# 3 Technical Overview

## 3.1 The Browser: Zero Client

To overcome many of the short-comings of client side VPN solutions, the awayWEB systems utilises standard web browser technologies. The use of a web browser as a VPN client has a number of key advantages:

- Internet browsers are already installed in almost every Internet connected device, and configured for general Internet access
- Internet browsers work in a wide variety of network configurations. This includes operation from behind a corporate firewalls and through Internet proxies or other security systems.
- Internet browser availability is not restricted to particular operating system or platform. Therefore users with any version of Windows, Macintosh, PDA’s, WAP phones or other Internet appliances have access to suitable software.

## 3.2 Strong Client Privacy

Internet browsers are not specifically designed for security applications. The awayWEB system provides a number of security and privacy management features to protect the user and their sensitive information. The awayWEB system addresses browser privacy and security issues including :

- Browser History Snooping
- Cache Snooping
- Keyboard Sniffing

### 3.2.1 Browser History Snooping

During any given Internet session using a standard browser (e.g. Internet Explorer or Netscape) a concise history of pages visited is stored within the browser. Therefore anyone could obtain valuable information by inspecting the browser history after a user has closed their Internet session. The awayWEB system ensures that the names of the web pages visited using awayWEB are not retrievable once the session is completed.

### 3.2.2 Cache Snooping

Using a standard browser a cached copy of page content may be stored on the local machine. Therefore users may inadvertently leave sensitive corporate information on machines that they have used to browse the corporate network. Using the awayWEB system, the browser is automatically requested not to save copies of any information in the cache, regardless of the application or user settings.

### 3.2.3 Keyboard Sniffing

Many environments, such as Internet cafés, should be considered “hostile environments”. It is not unusual to discover that machines within these environments have had malicious software installed that looks for user names and passwords, and upon discovery sends them to a potential attacker. Using the awayWEB system, users within these “hostile environments” are protected from this type of attack (Section 3.4)

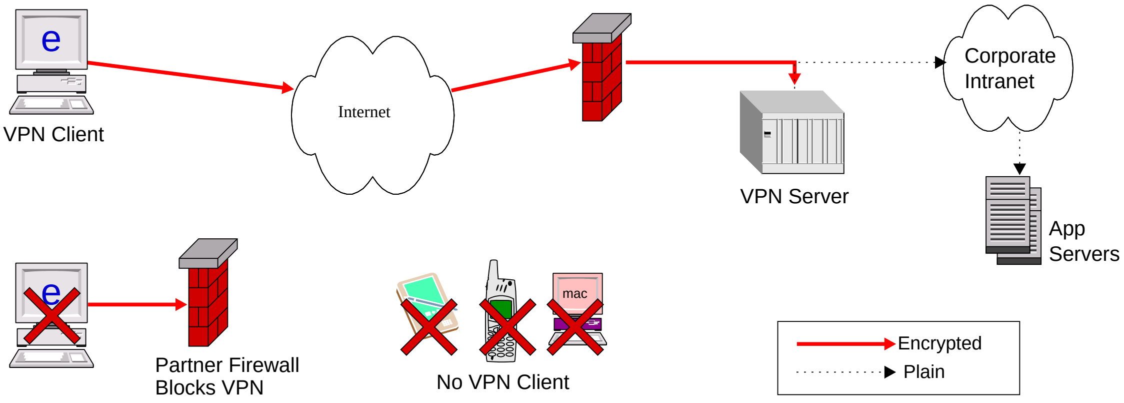


Figure 2: VPN's suffer restricted deployment

## 3.3 Strong Network Security

Almost all browsers support the Secure Socket Layer (SSL) standard. This standard is used extensively throughout the Internet to secure e-commerce transactions such as Internet Banking and Credit Card payments. The awayWEB system utilises SSL to ensure communications with the remote user remain private and secure.

AwayWEB is compatible with SSL web server security certificates (X.509v3) from all major certificate authorities, such as Verisign, Thawte, Entrust.net and Equifax. The use of X.509v3 certificates signed by recognised certificate authorities gives the users a high level of assurance that they are connecting securely to the appropriate corporate network.

AwayWEB supports full strength 128 bit encryption and is additionally compatible with Verisign 'SGC'/Global certificates.

## 3.4 Strong User Authentication

In the potentially "hostile environment" of the open Internet, the traditional username and password method of user authentication becomes dangerously ineffective. Passwords are easily stolen, copied or guessed by would-be intruders. The wide availability and usage of 'untrusted' public clients, such those found in airport lounge kiosks and Internet cafes makes the intruders life even simpler. Commonly available keyboard 'sniffing' software allows an intruder to easily steal network logon passwords entered into PC's in an Internet cafe.

To address this, awayWEB utilises 'two-factor authentication'. This is a system which ensures greater security than the traditional password by requiring two forms of identification. This is sometimes referred to as "has and knows", i.e. the user 'has' a physical object (such as a token) and the user 'knows' something (such as a pin-code to access the token). An example where this system is already widely used is for ATM transactions, which require both a bank card and a PIN for authorisation.

The awayWEB system supports a range of 'two-factor' authentication methods such as:

- SecurID,
- CryptoCard,
- Activcard,
- SafeWord
- and many others (Contact your awayWEB sales representative for more information)

Figure 3: RSA SecurID tokens

Hand-held authenticator tokens can be used with any computer system without requiring new software or additional hardware or peripherals to be installed or configured.

Each passcode provided by these tokens is valid only for a single use within a short period of time. Therefore a stolen password is useless, and it is impossible for users to write down or record their password in in-appropriate locations.

With these devices it becomes difficult for users to misuse their login name and passwords. Unlike traditional login names and passwords, tokens must be used with their associated pin codes. This high level identity assurance can also offer an aspect of 'non-repudiation'.

### 3.5 Centralised Authorisation & Access Control

The awayWEB system leverages existing investment in infrastructure, policies and support arrangements by accessing the existing authorisation infrastructure. Once users are authenticated, the permissions and privileges granted to each user are controlled using a central authorisation policy and authorisation database.

The awayWEB system uses the standard LDAP protocol to access a directory of users and their associated group memberships. AwayWEB works with:

- Active Directory,
- Novell Directory Service (NDS),
- I-Planet directory server,
- and others - contact your awayWEB sales representative for more information.

The authorisation database is used to enforce access controls within the awayWEB system based upon each user's membership to different groups within the directory. The access control system is powerful enough to allow you to allocate group memberships to business partners and create an 'extranet' which allows only specific partners to access specific pages of an internal application.

### 3.6 Centralised Audit

The awayWEB system records an audit trail of every intranet action taken by each remote user. The use of strong, two-factor authentication means that each user can be held accountable for the actions logged against their identity. In the event that an intranet system is mis-used, the awayWEB gateway provides a strong independent audit-trail of all activity.

As a minimum the audit trail records the following information, for each HTTP request processed:

- Date & Time of access
- Source IP address of access
- The username associated with the access
- Type of browser used for the access
- Full URL of the accessed intranet system, including any query parameters
- Whether the access was allowed or denied by the awayWEB system
- The size (in bytes) of the intranet server's response
- The 'Subscriber ID' for WAP users when provided by a WAP gateway

This audit trail is stored in 'Extended Common Log Format', which is compatible with all standard web server reporting and analysing tools.

## 4 HAT: Hypertext Address Translation

The awayWEB system provides a secured central control point for all access to intranet services. The system enables all intranet services to be presented as a single, secured, web server on the Internet.

This is achieved through 'Hypertext Address Translation' (HAT). As each intranet request is serviced by the awayWEB system, the HTML content of each page is examined and every hypertext link is modified by the awayWEB system. The links are extracted and re-written so that every link on the page is a link to a location on the awayWEB system. No matter what link is chosen by the user, it points to the awayWEB system, not directly to any intranet site.

When the awayWEB system receives a request for a link, it re-translates the intranet link, checks the users' authorisation and fetches the correct content from the original intranet server. As this content is retrieved and forwarded to the client, the links are again translated.

All intranet URLs are translated to URLs on the awayWEB gateway, so that internal systems can share the security and encryption features through a single Internet connection.

Example intranet and Internet URLs are shown in table 1.

## 5 Fine Grained Access Control: URL based rules

Access to intranet resources is controlled according to the administrative security policy defined in the awayWEB system. The policy specifies the access control rules in terms of which users and groups may access which internal URLs by matching the URL from each user request with a list of URL patterns defined by the policy ruleset.

The awayWEB URL mechanism is far more powerful than access control mechanism implemented within firewall rule sets. Every element of the URL in each request may be used as part of the access control rule. Therefore very fine-grained control is possible over which users have what level of access. The rule matching allows the scope of a rule to be as broad as 'allow all authorised users to access all intranet hosts', down to very specific rules such as 'deny access to all *.xls files to all users not in the "Finance" group'. This is not possible with conventional IP based filter rules supplied by firewall applications.

| URLs of intranet pages | URLs after HAT (Sent to the remote browser) |
|---|---|
| http://intranet.finance.example.com | *https*://awayweb.example.com/p/s/http%3a//intranet.finance.example.com |
| index.html | https://awayweb.example.com/p/s/http%3a//intranet.finance.example.com/index.html |
| sales/2001.html | https://awayweb.example.com/p/s/http%3a//intranet.finance.example.com/sales/2001.html |
| *Same URL with URL encryption feature enabled* | https://awayweb.example.com/p/s/P98jA(86a99976vd699a8dhn9m(dFUTFhtgYTF/X/X |

Table 1: URLs before and after HAT

These fine grained controls cover most features in the server - such as the privacy enforcement policy, URL encryption, cache control and compression (8.2). This allows the same flexibility of control for all aspects of the server configuration - for example, rules as powerful as ’use dynamic compression for all users in the “Modem Users” group when accessing ’*.doc’ files on any server in the ’*.office.example.com’ domain” can be configured if required.

## 5.1 Ordering

The use of strict ’top-to-bottom’ ordering of the awayWEB policy rules allows for a compact and powerful expression of an organisations security policy. This generally requires very little maintenance therefore reducing overhead costs. Exceptions can be configured before a more general rule, rather than requiring endless lists of specific policies - for example:

1. Allow access to ’http://sales.intranet.example.com/’ to the “Sales” group
2. Deny access to ’http://sales.intranet.example.com/’ to everyone
3. Allow access to ’http://*.intranet.example.com/’ to everyone
4. Deny all access to everything else

By following the policy rules from top to bottom, it is clear that the “Sales” group has extra access permission, without requiring the rules to list each and every intranet server in the organisation.

## 5.2 Regular Expressions

The URL matching performed by the awayWEB system is based on patterns. This allows multiple servers or web pages to be grouped into a single rule.

The awayWEB system utilises a powerful pattern matching tool called “regular expressions”. Below is an example of the power of pattern matching . The rules below can be used to allow some users to access a general intranet application, but only allow access when specific application parameters (such as account numbers) are used, and deny any other access:

1. Allow access to
   http://finance.example.com/balance.asp?account=B1234[0-9]
   to the “Company B” group

2. Deny all access to everything else to the “Company B” group

3. Allow access to
   http://finance.example.com/balance.asp?account=*
   to the “Finance” group

Here, the users from “Company B” can only see their own account balances, B12340 through to B12349, but the “Finance” group can see all account balances.

## 5.3 Security URL Normalisation

An important security feature of the awayWEB system is the ’URL Normalisation’ system. The use of pattern matching to allow or deny access is very powerful, but any individual web page can often be accessed in a multitude of different ways. Many different forms of a URL are recognised as equal by most web servers. Most elements of the URL have multiple possible formats, for example:

- Any special characters can also be expressed using ’URL Escaping’, which replaces the special character with a ’%’ mark and a character code.
- Paths can include ’..’ to ’back up’ a level before continuing
- The site name and scheme can be in upper or lower case
- The port number is optional for port 80 and 443

Therefore:

- HtTp://Sales.Intranet.Example.COM/results.htm
- http://sales.intranet.example.com/folder/../results.htm
- http://sales.Intranet.example.com:80/folder/%2e%2E/results.htm
- http://sales.intranet.example.com:80/%72%65%73%75%6c
  %74%73%2e%68%74%6d

all refer to the same page. The access control rules must be able to match all the different forms to prevent ’back door’ holes in the security policy. The awayWEB gateway performs a sequence of ’normalisations’ on each URL before checking the policy for matches. All of the above variations are converted to the ’simplest’ form “http://sales.intranet.example.com/results.htm” before being checked against the rules.

# 6 Privacy Enforcement: The Details

## 6.1 URL Encryption

Web browsers store a history of URLs that the user has visited during any given browsing session. Once a user quits the browser, the history remains and can be examined by any future user of the PC. URLs from a corporate intranet may contain information that is of interest to attackers. This information may include the names of internal servers, the names of directories and folders on those servers and the names of individual pages. Leaving such information on an unprotected public PC in an Internet cafe should be regarded as a security risk. (Figure 4)

The AwayWEB system uses ’URL encryption’ to eliminate this risk. As the awayWEB system performs the HAT function (section 1), it encrypts the URL into a meaningless string before it is sent to the client browser. This string is meaningless to all but the originating awayWEB system, where is it used to recover the original intranet URL.

## 6.2 Title Privacy

Each entry in the ’history’ of a browser normally records not only the URL of a page, but also the ’<TITLE>’ element assigned to the page. The list of page titles is in itself a valuable source of corporate information. Commonly, titles will include the names of documents viewed, the subjects of emails or the results of data entry on an internal system.

AwayWEB is configured to remove the <TITLE> elements from each page as content goes through the HAT process. The result is that the browser history no longer records the title of each page. When combined with the URL encryption feature, the history shows only scrambled URLs and blank page titles. (Figure 5)

## 6.3 Cache Control

Browser clients make heavy use of local caching of HTML, images and other content to improve the speed of Internet browsing. This is desirable for general Internet browsing, but it represents a privacy risk to confidential corporate information. Intranet documents that are stored in the cache of the browser are written to the hard disk of the client machine and remain accessible once the user has logged out. These files remain accessible to any subsequent user of the PC, for an indefinite period of time.

Web applications have the ability to instruct the client browser that particular content is not be stored in the cache. Each applications must be specifically written or modified to send the appropriate control information. Often it is difficult or impossible to configure this feature for static content (such as plain HTML pages and images).

The awayWEB system can add the required Cache Control information to all content as it passes through the system. This Cache Control information instructs the browser to not cache content on the local hard disk. This reduces the risk of disclosure once the user session is completed.

Preventing caching of all content could have adverse affects on web site performance, especially if the site is designed with graphical interface or utilises a large number of icons, bullets or other images for decoration. In order to minimise performance impact, the awayWEB system can be configured to allow or deny caching of images based upon their file size. For example, small images less than 2k could cached, as they are probably buttons and icons, whereas large images greater than 2k are probably important diagrams, charts or photographs, and should therefore not be cached.

# 7 Sign-On Minimisation

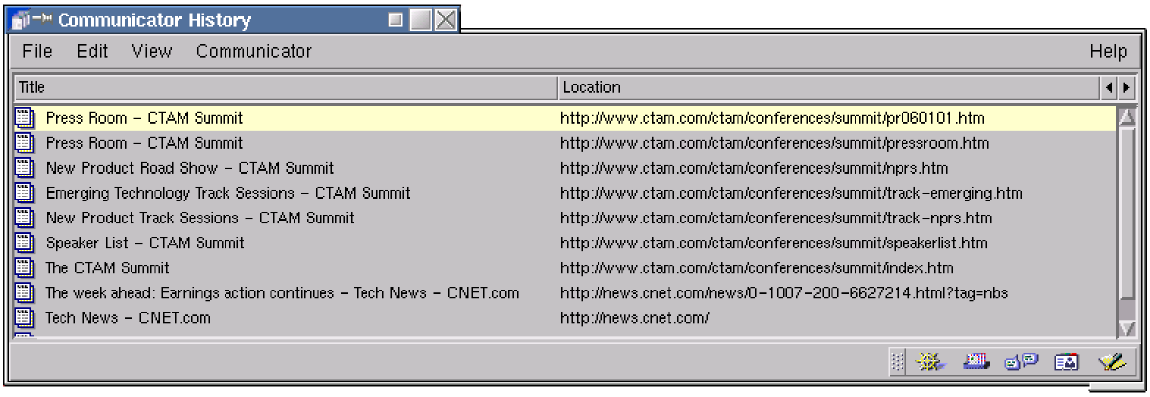
Once users are authenticated to the awayWEB gateway, they may access intranet systems as if they were directly connected to the organisation network (subject to the access control policy).

Each intranet system may have its own authentication requirements and each internal authentication system may operate using a variety of common web authentication schemes.

Using a variety of techniques, awayWEB can greatly reduce or completely eliminate the need for repeated logins.

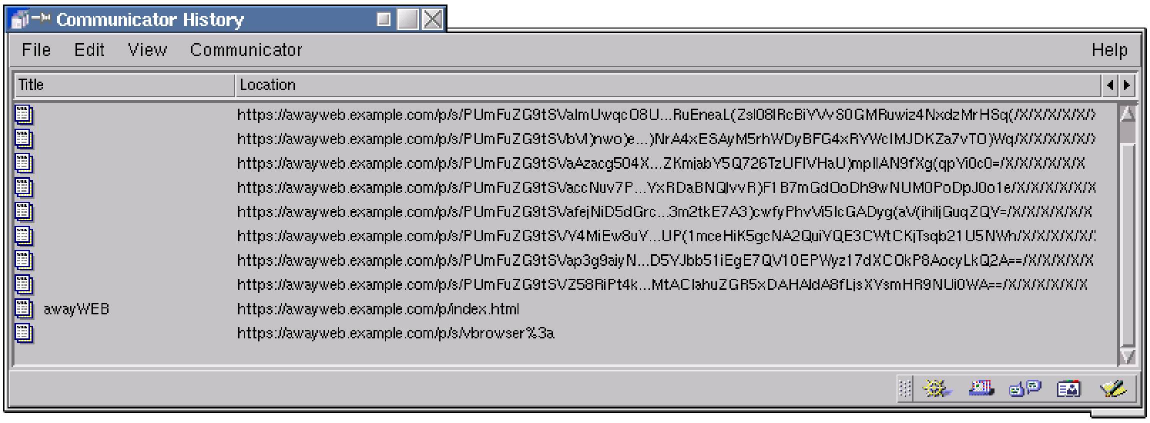
## 7.1 Credential Storage

Rather than sending user authentication information to the browser the awayWEB system uses both a “cookie storage” system (see 8.1) and a ’Credential Store’ to save user login and session information at the gateway. Users login information is preserved in the gateway even when a user is logged out of awayWEB. When a user re-connects at a later time, they can continue with their intranet applications without repeating the login process. (This functionality is subject to login time limits or other policy enforced by the intranet system). This provides a number of important benefits:



| Title | Location |
|---|---|
| Press Room – CTAM Summit | http://www.ctam.com/ctam/conferences/summit/pr060101.htm |
| Press Room – CTAM Summit | http://www.ctam.com/ctam/conferences/summit/pressroom.htm |
| New Product Road Show – CTAM Summit | http://www.ctam.com/ctam/conferences/summit/nprs.htm |
| Emerging Technology Track Sessions – CTAM Summit | http://www.ctam.com/ctam/conferences/summit/track-emerging.htm |
| New Product Track Sessions – CTAM Summit | http://www.ctam.com/ctam/conferences/summit/track-nprs.htm |
| Speaker List – CTAM Summit | http://www.ctam.com/ctam/conferences/summit/speakerlist.htm |
| The CTAM Summit | http://www.ctam.com/ctam/conferences/summit/index.htm |
| The week ahead: Earnings action continues – Tech News – CNET.com | http://news.cnet.com/news/0-1007-200-6627214.html?tag=nbs |
| Tech News – CNET.com | http://news.cnet.com/ |

Figure 4: Typical Browser History



| Title | Location |
|---|---|
| | https://awayweb.example.com/p/s/PUmFuZG9tSValmUwqcO8U...RuEneaL(ZsI08IRcBiYVvS0GMRuwiz4NxdzMrHSq(/X/X/X/X/X/ |
| | https://awayweb.example.com/p/s/PUmFuZG9tSVbVl)nwo)e...)NrA4xESAyM5rhWDyBFG4xRYWcIMJDKZa7vTO)Wq/X/X/X/X/X/ |
| | https://awayweb.example.com/p/s/PUmFuZG9tSVaAzacg504X...ZKmjabY5Q726TzUFIVHaU)mpIlAN9fXg(qpVi0c0=/X/X/X/X/X/X |
| | https://awayweb.example.com/p/s/PUmFuZG9tSVaccNuv7P...YxRDaBNQlvvR)F1B7mGdOoDh9wNUM0PoDpJ0o1e/X/X/X/X/X/X |
| | https://awayweb.example.com/p/s/PUmFuZG9tSVafejNiD5dGrc...3m2tkE7A3)cwfyPhvVi5IcGADyg(aV(ihiljGuqZQY=/X/X/X/X/X/X |
| | https://awayweb.example.com/p/s/PUmFuZG9tSVY4MiEw8uY...UP(1mceHiK5gcNA2QuiYQE3CWtCKjTsqb21U5NWh/X/X/X/X/X/ |
| | https://awayweb.example.com/p/s/PUmFuZG9tSVap3g9aiyN...D5YJbb51iEgE7QV10EPWyz17dXCOkP8AocyLkQ2A==/X/X/X/X/X |
| | https://awayweb.example.com/p/s/PUmFuZG9tSVZ58RiPt4k...MtAClahuZGR5xDAHAldA8fLjsXYsmHR9NUi0WA==/X/X/X/X/X/X |
| awayWEB | https://awayweb.example.com/p/index.html |
| | https://awayweb.example.com/p/s/vbrowser%3a |

Figure 5: Browser History protected by awayWEB

- Once a user has logged in to an intranet system once, they need never log in again thus reducing the number of user sign-ons required.

- Internal passwords are not used in the untrusted environment. The user never needs to type intranet passwords into the keyboard in an Internet cafe or other unsafe environment

- Reduced data entry in WAP applications minimising or eliminating difficult user name and password entry on small devices like WAP phones

### 7.2 Intranet Single Sign-On

If your organisation already employs a single sign-on system for intranet applications, users need only perform a single intranet sign-on to remain permanently authenticated (subject to your SSO system policies). The awayWEB system will operate automatically with most single sign-on system that inter-operate with a standard browser.

### 7.3 Intranet Zero Sign-On

The awayWEB system can be configured to pass the credentials of each user to an internal system by appending an additional HTTP credential header to each intranet request.

The intranet system can easily access the additional information and use it to customise site content or preferences. For secure applications, the user id can be used for a system login. This information is protected by a timestamp and a digital signature. Through the use of plug-in modules for supported web server the intranet system can validate the signature to ensure that only the awayWEB gateway can perform the secure login.

## 8 Additional Features

### 8.1 Cookie Storage

Many intranet applications make use of ’cookies’ for storage of user-specific information. Information such as:

- Personal Information
- Site Preferences
- Default Selections
- Previous Query Results
- Security and Login Credentials
- Login Session Keys

The above information stored in cookies may be both private and confidential, or useful to the user. This information may be placed into cookies and stored in the users web browser cache on untrusted machines, either temporarily or for an extended period. To prevent this information from being stored in the untrusted web browser environment, and to prevent settings such as preferences being lost each time a user changes from one browser to another, the awayWEB intercepts all cookies from intranet sites, stores them only in the awayWEB system. Therefore none of this information is ever sent to the browser.

As a user browses the intranet, appropriate cookies are reattached to each request and passed back to the relevant intranet systems, allowing the preferences and credentials to be seamlessly retained between sessions.

This storage system also provides an additional security benefit. Cookies which have security significance, or are trusted by un-secured intranet applications, are never sent to or accepted from the client system. This prevents these cookies from being manipulated or misused by the end user, a common method of web site intrusions.s

### 8.2 Dynamic gzip Compression

The awayWEB system provides dynamic compression of web content passing through the server. All suitable content (HTML, Word documents, Text files etc.) can be automatically compressed to between 2 and 10 times smaller than its original size before being encrypted and passed to the client browser.

This feature uses the standard ’Content-Encoding’ feature supported by all modern web browsers, and requires no extra software or configuration of the client system. The feature is available to any web server or application which is specially modified to make use of it, but no current standard web servers support the system by default. With awayWEB system in place, all intranet systems immediately benefit.

Benefits of this dynamic compress feature include:

- Faster browsing experience and download speeds for users

- Removes performance loss due to SSL encryption often experienced by modem/dialup users

- Reduces data transfer charges and link utilisation which speeds access for all users

### 8.3 Intranet HTTPS

The awayWEB system supports the use https (SSL) encryption within the intranet, for additional application security. The intranet servers do not have to be configured

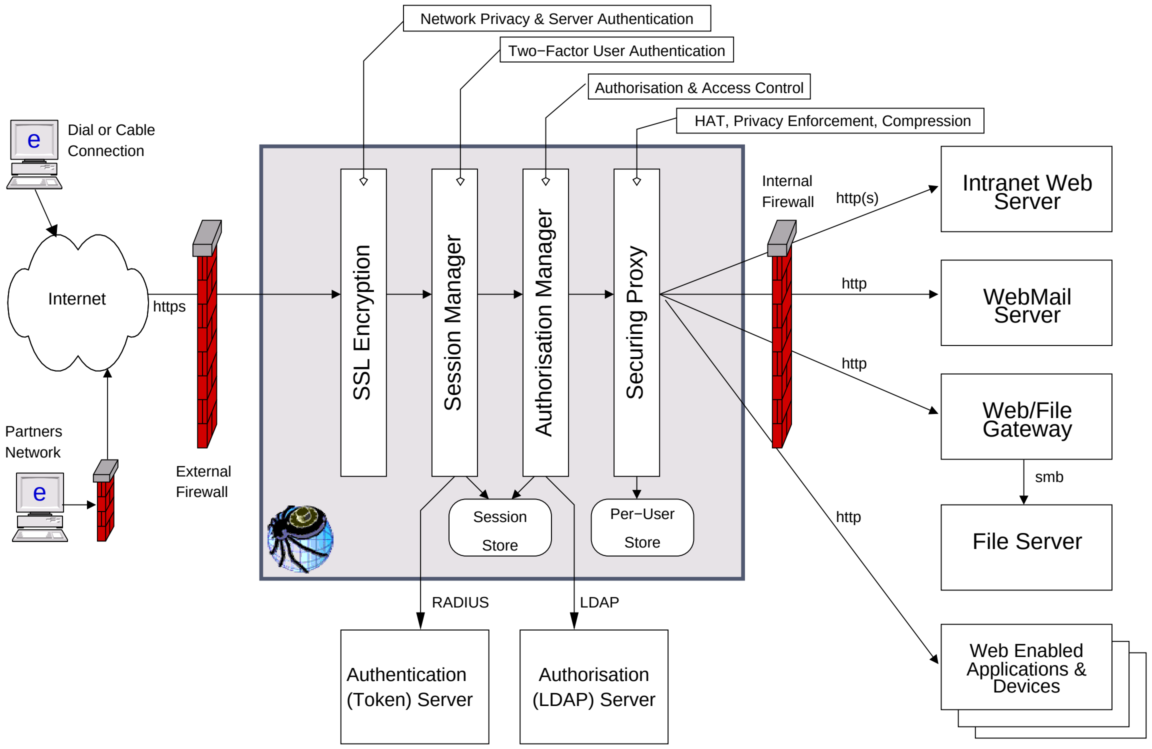


Figure 6: awayWEB Gateway - Internal Architecture

with SSL certificates signed by a public certificate authority. The awayWEB system accepts any internal CA certificate, or self-signed certificates may be used if preferred.

# 9 Internal Architecture Details

Figure 6 shows an overview of the internal architecture of the gateway system. Whilst the internal processing of the gateway is complex, the end user sees only a single simple login screen before being connected to their familiar intranet services.

The powerful and concise policy system, combined with integration with existing standards based authentication and authorisation systems (using RADIUS and LDAP), means that once configured, there is minimal additional administration overhead involved. No user accounts are manually created or managed in the system, and no routine administration is required for gateway operation.

# 10 WAP specific Features

WAP is a standard Internet protocol which has been designed to optimise the delivery of web based information to wireless and low-power computing devices, such as mobile phones and PDAs. The awayWEB system supports the WAP specific 'WML' content format used to deliver pages of information to WAP clients. WAP clients can log in to the awayWEB system, using two-factor authentication and their WAP client. Once logged in, users can proceed to access intranet content according to the access-control rules in the gateway.

## 10.1 WAP Security

WAP systems are designed so that client devices must access the general Internet through a WAP gateway server. The gateway server performs various network functions for the WAP device which would otherwise consume too many resources in the client. These services include translation between HTTP and the WAP specific WSP protocol, managing cookies and bookmarks, history and user preferences. The delegation of these functions from the client to the WAP gateway server raises security issues when accessing intranet services through the gateway.

By default, WAP applications enjoy very little security protection from the WAP infrastructure (Figure 7). By employing best practice security techniques, the awayWEB system can greatly improve the end-to-end security of WAP applications (Figure 8).

A specific service provided by the WAP gateway is the translation of WAP specific WTLS encryption into industry standard SSL encryption for access to 'https' protected web content. The WAP gateway has full access to the content of each request - the use of WTLS and SSL encryption does not protect information whilst it is passing through the

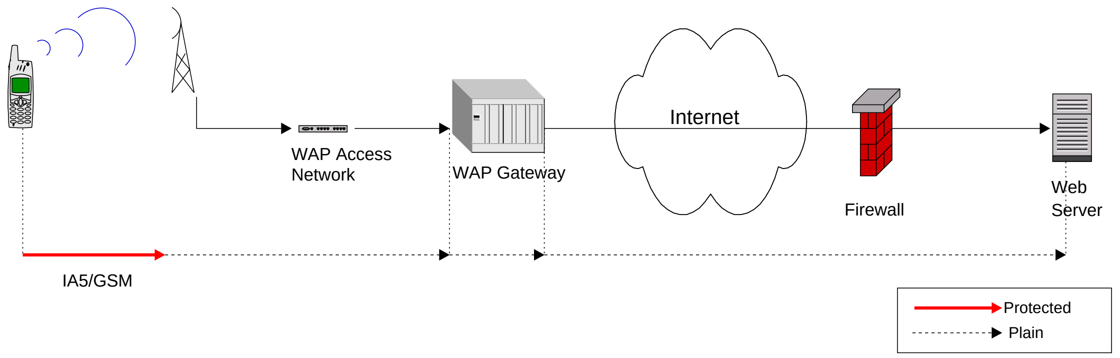


Figure 7: Security protection in 'default' WAP deployments

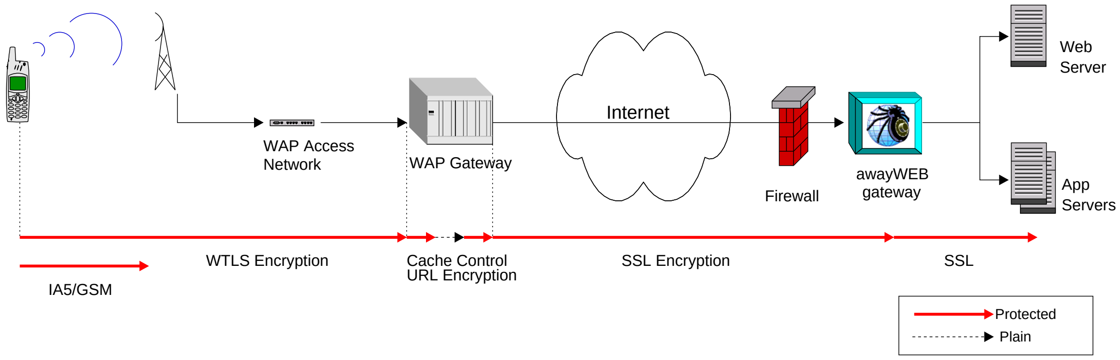


Figure 8: Best Practice Security protection in awayWEB WAP

WAP gateway itself (Shown by the unprotected communications illustrated in the WAP gateway in figure 8).

The WAP gateway should, therefore, be operated by a trusted party if sensitive corporate information is passed through it. An organisation which wishes to use WAP but prefers to avoid installing its own WAP-specific infrastructure should ensure it selects a WAP gateway provider (often the mobile phone service provider) which offers a sufficient level of security assurance.

Certain security issues remain even if the normal operation of the WAP gateway is not compromised - in particular, certain corporate information is likely to be recorded by the WAP gateway, subjecting it to the risk of unauthorised disclosure. These risks are similar to those experienced by browsers in un-trusted environments (and are mitigated in similar ways) except that the exposure is at the WAP gateway, rather than in the client system.

### 10.1.1 Gateway History Access

The WAP gateway maintains a history of URLs accessed by each client. This may include information about intranet systems, names of documents and parameters provided to intranet applications. This risk is mitigated by the same awayWEB feature that provides privacy protection in the HTML environment: URL encryption. (See 6.1) Intranet content is modified by the awayWEB gateway so that the details of each link are encrypted and meaningless to the WAP gateway. When the encrypted link is accessed, an authorised user can obtain the appropriate intranet content, but the records of the WAP gateway will show only the encrypted URL information. This minimises the risk of misuse by the WAP gateway operator.

The audit trail recorded by the awayWEB gateway (available only to the awayWEB administrator) shows each full, un-encrypted intranet URL that was actually requested by the client (along with WAP-specific information, such as the WAP subscriber number).

### 10.1.2 Gateway Cache Control

Most WAP clients (such as mobile phones) have very limited memory. In order to speed up browsing of commonly requested content, the WAP gateway server usually caches copies of each page requested by the client. The copies may remain on the WAP gateway for an indefinite period (often up to 30 days), during which time they may be accessed either by an intruder or the administrators of the server. WAP applications can signal to the WAP gateway not to cache such information, but this involves modifying each application during development to send the correct signals (HTTP headers). The awayWEB gateway can add the appropriate cache-control headers to each intranet page before it is sent to the WAP gateway, without requiring changes to the intranet applications. The same cache-control mechanism used to provide privacy protection for HTML browsers (see 6.3) operates at the WAP gateway.

## 10.2 WAP Usability

WAP devices often have very limited functions for data-entry. The use of a mobile phone keypad makes careful design of WAP displays and minimisation of user input very important for usability of WAP applications.

AwayWEB maximises WAP usability in a number of ways:

### 10.2.1 Custom login templates

awayWEB is supplied with a variety of login form templates tuned for specific brands of token card. For example, the RSA SecurID card produces an 'all-numeric' passcode - the awayWEB login page can use this feature to automatically force the phone into 'number entry' mode - this can cut down the required number of user keystrokes by up to 75% during a typical login.

### 10.2.2 Username caching

As users usually use the same mobile phone, awayWEB can 'pre-fill' the username field on the phone/PDA with the last username used, saving the need for multiple entry. This can reduce keystrokes by 50% compared to a system which required the username to be completed on each login.

### 10.2.3 Single & Minimised sign on

The awayWEB sign on minimisation features (See section 7) are a major benefit to WAP users, who may otherwise need to log in separately to multiple intranet applications.

# Copyright & Trademark Information

Level 21, 201 Miller St,
North Sydney NSW 2060
Australia

SecurID, ACE Server are trademarks or registered trademarks of RSA Security Inc.

Microsoft, Active Directory, Internet Explorer are trademarks or registered trademarks of Microsoft Corporation

Macintosh is a trademark or registered trademark of Apple Corporation

NDS is a trademark or registered trademark of Novell Inc.

I-Planet is a trademark or registered trademark of Sun/Netscape Alliance

CryptoCard is a trademark or registered trademark of CryptoCard Corporation

ActivCard is a trademark or registered trademark of ActivCard

SafeWord is a trademark or registered trademark of Secure Computing Corporation

# Disclaimer of Warranties

/dev/secure Pty Ltd & awayWEB (Aust) Pty Ltd makes all reasonable efforts to ensure that information contained in this document is accurate. However, we makes no warranties as to the accuracy or completeness of this information and disclaims all warranties, express or implied, including, but not limited to, warranties of merchantability, fitness for a particular purpose, and non-infringement. This document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein; these changes will be incorporated in new editions of the document. We may make improvements and/or changes in the product(s) and/or the program(s) described in this document at any time. In no event will /dev/secure Pty Ltd or awayWEB (Aust) Pty Ltd be liable for any loss arising as a result of inaccuracy or incompleteness of information in this document.

$Id: architecture-overview-whitepaper.lyx,v 1.1.1.1 2001/08/20 04:49:25 cbailiff Exp $