



Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Options For Securely Deploying Outlook Web Access

Outlook Web Access, or OWA, allows users to access their Exchange email via a web browser and Internet connection. Considering the growing trend of remote offices, 'road warriors' and work-from-home staffing options, Outlook Web Access can greatly enhance the efficiency and productivity of corporate employees. However, OWA is not a simple solution. There are many aspects to consider prior to deploying Outlook Web Access. Broad considerations include: What is your current internal architecture? How secure do your commun...

Copyright SANS Institute
Author Retains Full Rights

AD

A banner advertisement for FireEye. On the left is the FireEye logo, which consists of a stylized red and white eye with a flame-like shape above it. To the right of the logo, the text reads: "Protect critical data from the cyber theft pandemic." in red and white, followed by "Learn how in this FireEye white paper." in white. The background of the banner is dark and features a man in a hard hat looking at a computer screen with a yellow bird icon.

OPTIONS FOR SECURELY DEPLOYING OUTLOOK WEB ACCESS

ABSTRACT

Outlook Web Access, or OWA, allows users to access their Exchange email via a web browser and Internet connection. Considering the growing trend of remote offices, 'road warriors' and work-from-home staffing options, Outlook Web Access can greatly enhance the efficiency and productivity of corporate employees. However, OWA is not a simple solution. There are many aspects to consider prior to deploying Outlook Web Access. Broad considerations include: What is your current internal architecture? How secure do your communications need to be? Who will have the ability to use Outlook Web Access? How can OWA be deployed within your organization in accordance to your security needs assessment?

In this paper, I will provide an overview of Outlook Web Access and how it functions to deliver Exchange server mail via HTTP. Next, I will take an in-depth look at four primary areas of concern in securing OWA; 1) the foundation technology, 2) encryption and authentication, 3) network architecture and, 4) logoff.

Finally, I will review various products that offer a more secure way to deploy OWA than the off-the-shelf solution. It is my goal to heighten the reader's awareness of the potential security risks associated with Outlook Web Access and to provide sufficient technical information regarding options for securely deploying OWA such that administrators can make informed decisions to narrow the direction they wish to take their own deployment efforts. This paper is not an endorsement for any one product or solution.

WHAT IS OWA?

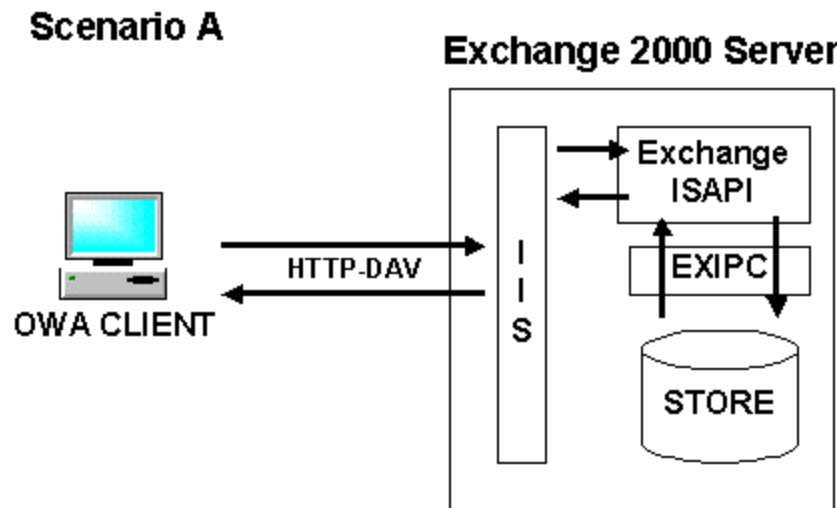
Outlook Web Access (OWA) offers a means for remote users to access their Exchange email via an HTTP connection. Outlook Web Access was first introduced as a feature of Exchange Server 5.0 and was greatly enhanced with the release of Exchange 2000. Some of the added features with the new 2000 release include the ability to use Outlook rules, spell checker, and tasks lists among others.

There are five basic steps to accessing Exchange mail via Outlook Web Access. First, an HTTP request is made from a web browser somewhere on the Internet to the IIS service running on an Exchange server. Next, the IIS server responds with an HTML based login page. In the third step, the user is authenticated in one of three methods; Basic Authentication, which includes a mailbox name, domain username and password, or Challenge/Response, where something the user knows, like a PIN, is combined with something they have, such as a token

number, or by SSL certificates. After a user is validated, MAPI, ASP and RPC data are converted to HTML and sent over the HTTP connection back to the client. Access to the users email, calendar and public folders is now established. When the user has completed their tasks, they must log off and close the browser to end their session.

(<http://www.microsoft.com/Exchange/en/55/help/default.asp?url=/Exchange/en/55/help/documents/server/xog18001.htm>)

One of the most basic deployments of an Outlook Web Access environment is diagramed below (Figure 1).



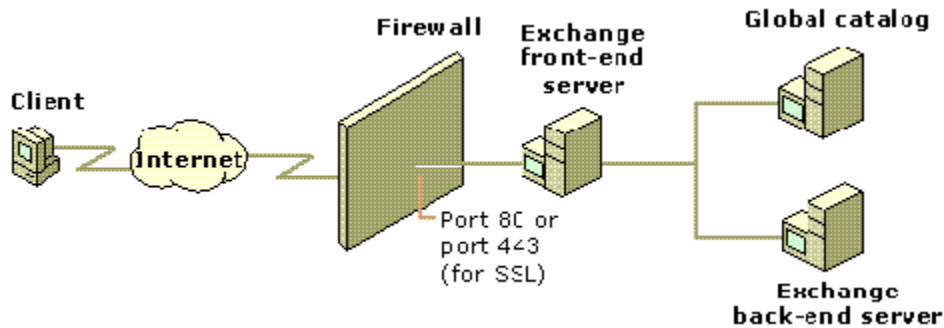
(Figure1) Scenario A is a basic, single-server scenario that illustrates the fundamental components of an OWA architecture. OWA clients connect directly to their mailbox server through IIS. When an OWA client request is received by IIS and the Exchange store is local to that server, EXIPC is used to retrieve the local data rapidly.

(http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/guide/plan/p_10_tt1.asp)

OWA 2000 relies on Microsoft's IIS 5.0 (Internet Information Server 5.0) to relay requests from a remote client to the Exchange server. In the above diagram, IIS resides on the same physical machine as the Exchange server and the Web Storage System. This design, while simple, is also a high security risk. The risks include exposing the IIS server directly to the Internet, the lack of SSL (Secure Socket Layer) for encrypting data, and the fact that the IIS server shares a physical location with both the Exchange server and the Web Storage System means that if the web server is compromised, the attacker has control of not one but three vital systems.

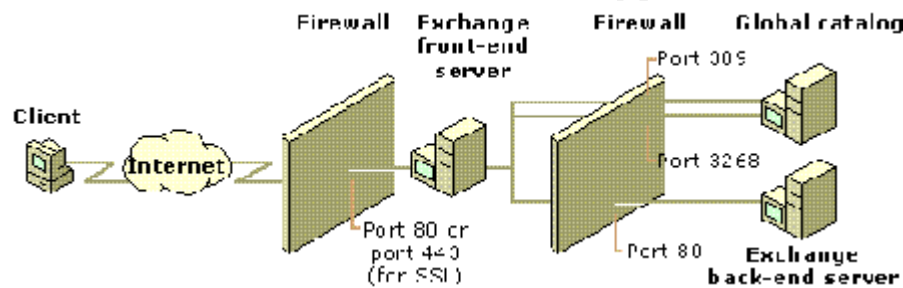
Outlook Web Access is installed automatically during an Exchange 2000 server installation. This install, as represented above, provides minimal security but may be a suitable option for an intranet deployment of OWA, however because of the substantial risks associated with this deployment, it would not be recommended for use on the Internet.

Adding firewalls and strategically positioning servers in secured subnets and DMZs can establish higher levels of security. Establishing defense in depth to an OWA deployment creates a more secure environment and fewer opportunities for exploitation. The two diagrams below provide a basic view of single and double firewall topologies.



(Figure 2) Single Firewall

Placing a firewall between the Internet client and the front-end server allows OWA clients to communicate with the server that uses the HTTP protocol and SSL (optional encryption) protocols. (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/guide/plan/p_10_tt1.asp)



(Figure 3) Perimeter Network (Two Firewalls)

In this option, the front-end server is on a perimeter network. The "outer" firewall protects the perimeter network from the Internet, and the "inner" firewall protects the private network from the perimeter network. (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/guide/plan/p_10_tt1.asp)

AUTHOR'S NOTE:

Because the terms DMZ and screened subnet are sometimes used interchangeably, the definition that I will adhere to is from "Inside Network Perimeter Security" where DMZ is defined as "an insecure area between secure areas" and screened subnet is defined as "an isolated network that is connected to a dedicated interface of a firewall or other filtering device." (Northcutt, et al; "Inside Network Perimeter Security" pg 6. 2003)

VULNERABILITIES

Since OWA is built upon both Internet Information Server and Exchange Server, it is subject to all of the many vulnerabilities associated with each of those individual products.

The effects of hackers exploiting vulnerabilities in IIS have been well publicized. In July 2001, the Code Red worm (versions 1 and 2) wreaked havoc. Within fourteen hours, almost 360,000 IIS web servers worldwide were infected with Code Red version 2. The worm exploited a buffer overflow vulnerability. "It allows system-level execution of code and thus presents a serious security risk. The buffer-overflow is exploitable because the ISAPI (Internet Server Application Program Interface) .ida (indexing service) filter fails to perform adequate bounds checking on its input buffers." (<http://www.caida.org/analysis/security/code-red/>)

In September 2001, IIS servers were again exploited. This time by another worm, Nimda. Nimda took advantage of no less than sixteen different flaws in IIS. (http://www.techprodx.com/pdfs/Email_Threat_Defenses.pdf page 10). One of those vulnerabilities, Web Server Folder Traversal, afforded a web site visitor the potential to do considerable damage to the site, including running unauthorized programs on it. (<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-078.asp>)

In April 2002, Microsoft released a cumulative patch to cover ten vulnerabilities in versions 4.0, 5.0 and 5.1 of the IIS servers. (<http://www.ciac.org/ciac/bulletins/m-066.shtml>). New patches and security enhancements continue to be released frequently.

Exchange server has its share of flaws as well. Microsoft Exchange 5.5 servers running Outlook Web Access service have a vulnerability that could reveal any email address within the Global Address List (GAL). This vulnerability exists in unpatched servers due to the ASP used by OWA to search the GAL does not require authentication. (<http://www.kb.cert.org/vuls/id/111947>)

Another vulnerability involves using Internet Explorer to access email via OWA and an Exchange 2000 server. A problem exists in the interaction between OWA and Internet Explorer when handling attached files. If a file is attached that contains HTML code that includes a script, the script will be run when the user opens the attachment. This occurs because OWA requires scripting to be enabled and the script can be executed against the users Exchange mailbox. (<http://support.microsoft.com/default.aspx?scid=kb;en-us;299535>)

In addition to the vulnerabilities of the core components of OWA, there are security risks associated with the network architecture in which it is deployed. Figure 2, above, diagrams a basic one-firewall deployment of OWA. In order to allow the front end OWA server to communicate with the back end Exchange server, at the minimum, port 80 needs to be opened. If SSL (Secure Socket Layer) is enabled, then port 443 also needs to be opened. If the front end server were to be compromised, the entire network would be at risk because there is

nothing to hinder an attacker once they have gained access to the front end server.

When a second firewall is introduced where the OWA server resides in a DMZ (demilitarized zone) and the Exchange server resides on the internal network, more ports need to be opened in order for the OWA server to communicate with the Domain Controller and the Exchange server. Port 135 is required for RPC (Remote Procedure Call) connection to the Exchange server. UDP ports 138 and 139 are required for connection to the Domain Controller (DC) and for user authentication.

(<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32&g=outlook+exchange+web+access> - pg 10 e-Gap Webmail appliance for MS Exchange free white paper)

Another possible deployment of OWA using Exchange 2000, is to enable OWA on an Exchange Front-End server within a DMZ while the Exchange Back-end server and Active Directory server reside on the internal network. Placing the Exchange front end server in a DMZ exposes it to direct attacks. Also, if any other server within that DMZ is compromised, it could be spoofed to appear as the Front-End server, thus enabling access to the Back-end Exchange server while bypassing any authentication process. Because the Front End server is a fully functional Exchange server, there are even more serious implications of it being compromised.

Numerous ports need to be opened in the firewalls for servers in this configuration to communicate properly. Port 80 is required for HTTP between the Front and Back end servers. LDAP requests to the Active Directory server require Port 389 (TCP and UDP). Kerberos Authentication would require port 88. In order for the Front End Server to obtain IP addresses for the Exchange Back End and AD, port 53 would need to be open for DNS lookups. If implicit logins are desired, then port 135 (RPC) and port 445 would need to be opened for RPC and Netlogon, respectively. And as in the first scenario, ports 1024 thru 65535 need to be open for outbound connections to the Front End Exchange server. If the Front End Exchange server were to offer additional services such as SMTP, POP3 or IMAP, even more ports would need to be opened in the firewalls. (<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32&g=outlook+exchange+web+access> - pg 12 e-Gap Webmail appliance for MS Exchange free white paper)

In either of the above deployments, if authentication is not taking place at the Domain Controller or Active Directory Server then additional ports would need to be opened for communication between the OWA server and the authentication server. For example, if an ACE server were located on the internal network for use with SecurID, then UDP port 5500 would need to be opened on the internal firewall as well. Additionally, ports 1024 thru 65535 must be available for outbound connections from the Exchange server to the OWA server.

(<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32&q=outlook+exchange+web+access> - pg 12 e-Gap Webmail appliance for MS Exchange free white paper)

Finally, any inherent weaknesses within the existing network, such as poorly configured firewalls or routers, or devices that are not up to date on security patches, could expose OWA and all internal servers to more aggressive hacking attempts.

The third area of security concerns is that of encryption and authentication. OWA provides for four authentication methods: Anonymous, Basic Authentication – clear text, Basic Authentication – Clear text over SSL and Windows NT Challenge Response (NTLM).

Anonymous access to OWA allows anyone with a browser and the correct URL to access the OWA system. Users are not prompted for a user name or password. Security concerns with this access include unfriendly visitors viewing the Global Address List and any folders configured for public access. Anonymous logon is not secure and all logging is for a 'guest' user.

Basic authentication requires a user to provide a valid NT domain user name and password. Basic authentication can be implemented with or without SSL. If SSL is not required, the user name and password are transmitted over the Internet in plain text. This would allow someone with a sniffer to capture the credentials and ultimately gain access to the users OWA account and all the folders and resources available to that user as well. If SSL is required, the credentials will be sent encrypted, thereby reducing the potential of compromise. However, since the user name and password are static in nature, there is the potential that they could be cracked.

The remaining method of authentication offered with OWA is Windows NT Challenge/Response (NTLM). NTLM is similar to basic authentication in that a valid username and password must be supplied, however, the credentials will be sent encrypted by default. One consideration for implementing NTLM is that it is only supported if IIS/OWA and the Exchange server are on the same computer. It is not supported if the services are split on two different boxes. Like basic encrypted authentication, NTLM credentials are static and subject to cracking. Also, not all browsers (ex. Netscape Navigator) will support NTLM. (http://www.microsoft.com/exchange/techinfo/planning/55/OWA55_DeployPlan.doc)

Hand in hand with authentication is encryption. If SSL is implemented with the certificate and key stored on the Internet facing server, it is possible that the cert and key could be compromised. If hackers obtained the cert/key, they could mimic legitimate corporate servers or simply use that information to by-pass authentication on the OWA server.

Data sent between a Front End Exchange server and a Back End Exchange server is unencrypted. If the network on which they reside is compromised, a hacker could listen and obtain access to corporate data and confidential information, including usernames and passwords and email addresses.

The fourth and final area of concern I will address is that of secure logoff. When a user logs off of OWA, their session does not automatically end. They must completely close their browser in order to terminate the session. Since credentials are cached in the browser, they may remain available even after the user logs out. This can occur even if the browser is closed if a browser session remains open. An example of this would be if a stock or news ticker remained running after the user closed the browser. This fact is of considerable concern for security since one of the primary purposes of OWA is to allow users to access email from anywhere, which often means from public computer kiosks or other publicly shared computers. In some situations, browsers on these public systems are configured so that they cannot be closed. Thus if a user logs out of OWA, someone else could simply use the browser's 'Back' button to gain access to the user's email box, as well as any other folders or systems the user has access to via OWA.

The exposure to the vulnerabilities in the core components, the necessity of opening additional firewall ports, the issue of plain text basic authentication or even encrypted authentication, along with the inability to fully terminate an OWA session makes one acutely aware of the need for security diligence when deploying Outlook Web Access. Fortunately, there are many products available to assist you in designing and implementing a more secure OWA environment.

SOLUTION OPTIONS

The decision of which additional product, if any, to use when designing your OWA environment is based on a number of factors; the level of security required as determined by a security needs assessment, the architecture of your current network, budgetary constraints, and of course personal preference. The following provides an overview of several different solutions for securing Outlook Web Access. I will briefly describe each product and how it works as well as how it addresses each of the four areas of security concerns. My goal is to assist you in narrowing your field of options for researching your own solution to secure OWA deployment.

e-Gap Webmail Appliance – Whale Communications

Whale Communications (<http://www.whalecommunications.com>) offers a product called "e-Gap Webmail Appliance". This solution provides a secure front end access point to an Exchange 5.5 or 2000 server without exposing that server or any other internal system to the Internet. Whale describes the product as "...an

application specific "SSL VPN," it is a cost-effective, rapidly deployable alternative to traditional VPNs."

(<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32>).

The e-Gap Webmail Appliance has the capability to address all four areas of security concern when deploying OWA.

The e-Gap Webmail Appliance is comprised of three parts, an external e-Gap Single Board Computer (SBC), an internal e-Gap SBC and an e-Gap switch. These can be three separate units or combined in one 4U box. The external SBC is a virtual web server and is the only IP address that is published on the Internet. A user initiates communication via a secure connection to the external SBC over the Internet. The external SBC receives the packets, strips the headers, leaving only encrypted data, which it passes to the e-Gap switch via a SCSI connection. The switch then disconnects from the external SBC and connects to the internal SBC and passes the data to the internal SBC via SCSI. The switch cannot be connected to both the internal and external e-Gap SBCs at the same time. The data is decrypted on the internal SBC, an encrypted session is established with the user and login page is returned to the user for authentication. The internal e-Gap SBC communicates with the designated authentication server to validate the user. Data that is sent via the e-Gap is inspected and compared against an established rule set to determine if it is legitimate or a potential or known threat. This process is described in detail on the Whale website.

(http://www.whalecommunications.com/site/SFunctions/Viewlets/2284.EN.ver1/d/ataflow3_viewlet.html)

The e-Gap Webmail Appliance addresses the issues of the vulnerabilities of OWA's foundation technologies (Internet Information Server and Exchange server) in several ways. No data is sent directly to the real web server until the user has been strongly authenticated. The filtering that takes place on the internal e-Gap server inspects packets for anomalies such as malformed URLs or HTTP headers, excessive URL length, unexpected parameters/methods or unexpected extensions.

It is important to note that because the e-Gap Webmail Appliance performs its user-request inspection within the air-gap-protected back-end network and before reaching the real OWA server, the application-level controls are not subject to manipulation by external hackers, and cannot be circumvented.

(<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32> Free white paper "e-Gap Webmail Appliance for MS Exchange" page 8.)

The Whale e-Gap Webmail Appliance addresses network architecture concerns by essentially insulating the real web server and the Exchange server from the Internet. The only interface exposed to the 'Net is the external e-Gap Single

Board Computer that houses the virtual web server. The OWA/Exchange server is located in a secure subnet. The authentication server and/or directory server also sit behind the e-Gap in a secure network.

(<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32>
Free white paper “e-Gap Webmail Appliance for MS Exchange”) The e-Gap switch ensures that no Internet generated TCP/IP sessions are established with the OWA/Exchange server. “The e-Gap Webmail Appliance allows only application-level information to flow into an organization's internal network -- without requiring the opening of any ports from the Internet or DMZ to the back office.”

(<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32>)

To address the concerns regarding authentication and encryption, e-Gap Webmail Appliance offers support for numerous authentication options, including RSA SecurID, Vasco Digipass®, RADIUS, Active Directory, LDAP, and PKI Client Certificates. These additional options offer the ability to increase the security of user logins. E-Gap can also be configured to require SSL from end to end so that no data is ever sent plain text.

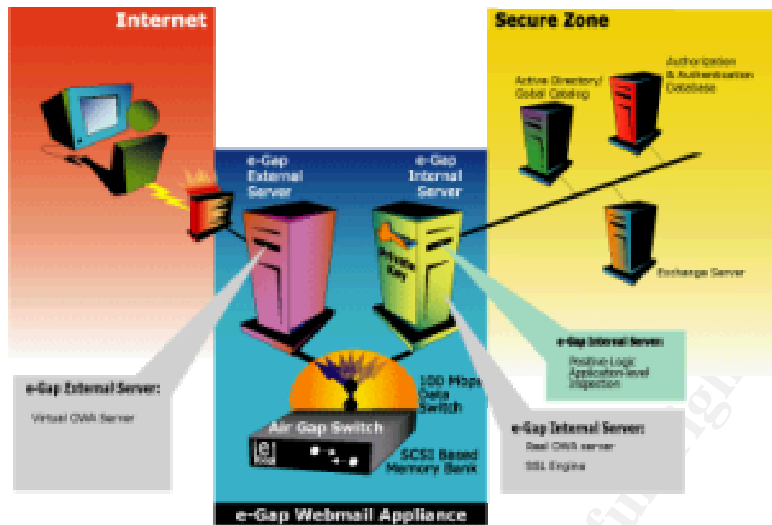
(<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32>
Free white paper “e-Gap Webmail Appliance for MS Exchange”)

The fourth concern, securing the log off process, is addressed by Whale's e-Gap solution by automatically breaking the authenticated session when a logoff is detected. This terminates the session fully thus preventing ‘back button’ re-entry to the OWA system. The e-Gap Webmail Appliance can also be configured with a timeout interval to force users to re-authenticate. If a user doesn't log out but simply leaves the browser open and walks away from the computer, someone coming in behind them will, at the predetermined interval, be required to re-authenticate.

(<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32>
Free white paper “e-Gap Webmail Appliance for MS Exchange”)

Whale also provides a demo of how the off-the-shelf log off method can be exploited. This can be viewed at http://www.whalecommunications.com/site/SFunctions/Viewlets/2282.EN.ver1/wbmailfinal_viewlet.html.

The diagram below is an example of how Whale e-Gap Webmail Appliance might be deployed.



<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32>

IronWebMail – CipherTrust

CipherTrust (www.ciphertrust.com) offers a module component to their IronMail product to help deploy a secure webmail solution. This module, called IronWebMail, functions as a secure proxy for OWA/Exchange. According to CipherTrust, “Ironmail [the parent product] is the first product designed to provide application level security for email.”

http://www.techprodx.com/pdfs/Email_Threat_Defenses.pdf pg 3

The IronWebMail module addresses all four areas of concern with regard to securing Outlook Web Access. By scrutinizing every connection to the web server, IronWebMail protects against exploits that utilize malformed URLs or path obfuscation. Protocol standards are also enforced. The administrator can set the maximum limits on URL characters to protect from POST or URL buffer overflow exploits. The number of directory transversals, as well as what directories can be transversed, are also configurable within IronWebMail. (<http://www.ciphertrust.com/ironmail/ironwebmail.htm>) IronWebMail contains an intrusion detection engine that detects and mitigates over 700 different web attacks. (http://www.nwtechusa.com/ironmail/secure_webmail.pdf page 4) This engine is an active IDS which not only observes an event but takes action to prevent it from becoming an incident.

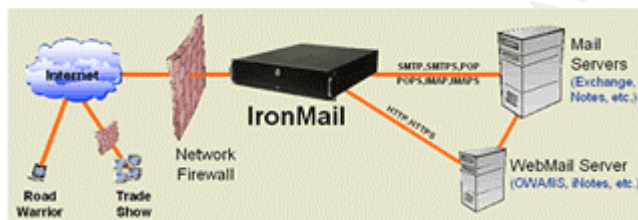
Unlike firewalls, IronWebMail can detect sequential packets containing malicious code. It will also detect and drop any unauthorized connections, logging all dropped connections. Because the IronWebMail appliance is the only device communicating directly to the Internet, fewer ports need to be opened in the firewall, thus reducing the exposure of the internal network to the outside world.

In the arena of authentication and encryption, IronWebMail offers a single sign-on option. The sign-on can be required to use a TLS (transport layer security protocol) tunnel to protect the username and password, thereby reducing the risk of interception by a hacker. IronWebMail also offers support for RSA SecurID and Strong Client Authentication (client-side certificates).

(http://www.nwtechusa.com/ironmail/secure_webmail.pdf)

IronWebMail can employ any one (or combination of) three different log off options, on-click, on session duration, and/or on session inactivity. Once a user clicks the OWA logoff button, IronWebMail automatically terminates the session. The session duration is a configurable value that will force a user to re-authenticate after a specified amount of time logged in. This capability helps reduce the time a third party might have for malicious work should the user leave the computer without logging off of their session. Another configurable value is session inactivity. If a connection is opened but remains inactive for a specified amount of time, IronWebMail will automatically terminate the session. Once the session is terminated, by which ever method, a new session cannot be established without another authenticated log on. 'Back button' usage will not re-enter the session. (http://www.nwtechusa.com/ironmail/secure_webmail.pdf)

An example of how IronWebMail might be integrated into a network is shown below.



(<http://www.locked.com/products/ciphertrust/ironwebmail.php>)

Alteon SSL Accelerator – Nortel Networks

Nortel Networks (www.nortelnetworks.com) offers a device called the Alteon SSL Accelerator. While the Alteon does not directly address the foundation technology security issues such as IIS and Exchange vulnerabilities, the Alteon removes the OWA/Exchange server from exposure to the Internet, thereby reducing the risk of attack. The Alteon does address several of the network and encryption/authentication concerns. No non-standard ports need to be opened on the firewall as the Alteon talks to the OWA/Exchange server on ports 80 and 443. Filters can be employed to restrict access and to detect and block known threats such as Nimda and Code Red. The use of filters can also aid in the reduction of spam mail.

(<http://www.nortelnetworks.com/products/01/alteon/isdssl/collateral/nn102560-112002.pdf>)

The Alteon SSL Accelerator handles all the SSL and PKI functions, which helps to increase web server performance. It reduces the risk of cert/key compromise by storing that data in an encrypted format. The Alteon offers support for X.509, LDAP, RADIUS and Exchange authentication methods.

(<http://www.nortelnetworks.com/products/01/alteon/isdssl/collateral/nn102560-112002.pdf>)

The Alteon SSL Accelerator does not address secure log-off.

There are many other solutions to offering a more secure Outlook Web Access deployment. The short list below is offered simply as an example of other options.

Secure Computing (www.securecomputing.com) offers PremierAccess. This is a part of their Safeword product and offers dynamic, token based authentication and access restriction to an OWA environment based on Access Control Lists. (<http://www.securecomputing.com/index.cfm?skey=643>)

Sun Microsystems (www.sun.com) offers Sun[tm] ONE Portal Server, Secure Remote Access 6. Secure Remote Access is a clientless VPN that allows for the encryption of all data between the client and the portal gateway. It also offers a URL re-writer to allow secure access to internal resources without publishing internal addresses. Support for both SSL and TLS is offered. For more information on this solution see http://www.sun.com/software/products/portal_sra/home_portal_sra.html.

SecureLogoff for Outlook Web Access is a solution offered by Messageware, Inc. (www.messageware.net). This software package allows the user to fully be logged off of OWA when clicking the logoff button. It clears all cached credentials and is supported by all browsers. It also offers security audit reporting. (http://www.messageware.net/products/securelogoff/ftp/SecureLogoff_Brochure.pdf)

CONCLUSION

As the number of road warriors, work-from-home employees and remote offices continues to increase, so does the need for communication between these employees and the home office. Outlook Web Access offers a viable method for remote or traveling employees to access their email, calendars and other important data without the additional expense of individual dial up accounts or client dependent VPN access. However, e-mail itself provides a target rich in sensitive information and sending that data over the Internet raises numerous security concerns. An off-the-shelf deployment of Outlook Web Access is riddled with security vulnerabilities by the very nature of the foundation technologies

upon which it is built, IIS and Exchange. These, along with other vulnerabilities, including network design and associated weaknesses, encryption and authentication concerns and insecure logoff methods, cause most administrators to steer clear of deploying this technology. There are solutions available, however, to assist in creating a more secure Outlook Web Access environment. These solutions range from very comprehensive, such as e-Gap WebMail from Whale Communications and IronWebMail from CipherTrust, to network based solutions including Nortels Alteon SSL Accelerator and Sun's Secure Remote Access server, to more targeted solutions like Secure Computing's PremierAccess or Messageware's SecureLogOff products. Depending on the security needs and budgetary constraints of your organization, one of these solutions may offer you the peace of mind to deploy Outlook Web Access for use within your enterprise.

POSTSCRIPT

In January 2003, Microsoft announced the newest release of Outlook Web Access and Exchange 2003. Some of the security added to this new release includes secure MIME, blocking automatic access to images, sounds and external contents and a special 'unblock' link to allow user discretion to access the above-mentioned resources. The ability to block attachments has also been added.

From the top 10 reasons to upgrade to Exchange 2003, "Greatly improved Outlook 11 and OWA performance that enables high productivity for mobile workers connecting over low-bandwidth, latent connections such as General Packet Radio Service (GPRS), 1xRTT, and dial-up connections."
(<http://www.microsoft.com/exchange/evaluation/ti/topten.asp>)

On January 7, 2003, Microsoft released Internet Security and Acceleration (ISA) Server 2000 Feature Pack 1. New functionality that is now offered includes URLScan, which works to prevent the use of the URL address space to exploit vulnerabilities on a server and support for RSA SecurID which will enable 2-factor strong authentication to the OWA server.
(<http://www.microsoft.com/isaserver/FeaturePack1/webandowa.asp>)

While this information is not included in the body of my paper, I felt it was important enough to the subject at hand to mention here.

REFERENCES

TEXT

Northcutt, Stephen; Zeltser, Lenny; Winters, Scott; Frederick, Karen Kent; Ritchey, Ronald W; "Inside Network Perimeter Security"; New Riders Publishing, Indianapolis, Indiana; 2003.

INTERNET

CipherTrust Home Page
www.ciphertrust.com (Jan 30, 2003)

CipherTrust, "Email Systems: Threats and Defense." April 19, 2002
http://www.techprodx.com/pdfs/Email_Threat_Defenses.pdf (Jan 12, 2003)

CipherTrust, "Ironmail Solution: IronWebMail"
<http://www.ciphertrust.com/ironmail/ironwebmail.htm> (Jan 30, 2003)

CipherTrust, "IronWebMail: Web Mail Protection"
http://www.nwtechusa.com/ironmail/secure_webmail.pdf (Jan 30, 2003)

Computer Incident Advisory Capability, "Information Bulletin." April 10, 2002
<http://www.ciac.org/ciac/bulletins/m-066.shtml> (Jan 20, 2003)

Cooperative Association for Internet Data Analysis, "CAIDA Analysis of Code-Red." Jan 30, 2003
<http://www.caida.org/analysis/security/code-red/> (Jan 3, 2003)

Lanza, Jeffrey P; CERT, "Vulnerability Note VU#111947." Sept 12, 2001
<http://www.kb.cert.org/vuls/id/111947> (Jan 10, 2003)

Messageware, Inc Home Page
<http://www.messageware.net> (Jan 3, 2003)

Messageware, Inc, "Secure Logoff for Outlook Web Access" 2002
http://www.messageware.net/products/securelogoff/ftp/SecureLogoff_Brochure.pdf (Jan 3, 2003)

Microsoft Corporation, "Microsoft Exchange Server 5.5." Feb 28, 2000
<http://www.microsoft.com/Exchange/en/55/help/default.asp?url=/Exchange/en/55/help/documents/server/xog18001.htm> (Jan 10, 2003)

Microsoft Corporation, "Planning Outlook Web Access Servers." 2003
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/guide/plan/p_10_tt1.asp (Jan 10, 2002)

Microsoft Corporation, "Microsoft Security Bulletin (MS00-078)." Oct 10, 2000
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-078.asp> (Jan 10, 2003)

Microsoft Corporation, "XGEN: Incorrect Attachment Processing in Exchange 2000 Outlook Web Access Can Run Script." Oct 16, 2002
<http://support.microsoft.com/default.aspx?scid=kb;en-us;299535> (Jan 20, 2003)

Microsoft Corporation, "Planning and Deploying Outlook Web Access 5.5."
http://www.microsoft.com/exchange/techinfo/planning/55/OWA55_DeployPlan.doc (Jan 12, 2003)

Microsoft Corporation, "Top 10 Reasons to Upgrade to Exchange Server 2003"
Jan 17, 2003
<http://www.microsoft.com/exchange/evaluation/ti/topten.asp> (Feb 8, 2003)

Microsoft Corporation, "Help Secure Web and OWA Servers." Jan 7, 2003
<http://www.microsoft.com/isaserver/FeaturePack1/webandowa.asp> (Feb 8, 2003)

Mission Critical Systems, Inc., "IronWebMail"
<http://www.locked.com/products/ciphertrust/ironwebmail.php> (Jan 3, 2003)

Nortel Networks, "Secure Remote Access to Email"
<http://www.nortelnetworks.com/products/01/alteon/isdssl/collateral/nn102560-112002.pdf> (Jan 1, 2003)

Secure Computing Home Page
www.securecomputing.com (Jan 3, 2003)

Secure Computing, "Safeword Premier Access"
<http://www.securecomputing.com/index.cfm?skey=643> (Jan 3, 2003)

Sun Microsystems Home Page
www.sun.com (Jan 3, 2003)

Sun Microsystems, "Sun ONE Portal Server, Secure Remote Access 6"
http://www.sun.com/software/products/portal_sra/home_portal_sra.html (Jan 3, 2003)

Whale Communications, "Home Page" 2002
<http://www.whalecommunications.com> (Jan 2, 2003)

Whale Communications, "e-Gap Webmail for MS Exchange."
<http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32&g=outlook+exchange+web+access> (Jan 1, 2003)

Whale Communications, "How Data Flows through the e-Gap System" 2002
[http://www.whalecommunications.com/site/SFunctions/Viewlets/2284.EN.ver1/da
taflow3_viewlet.html](http://www.whalecommunications.com/site/SFunctions/Viewlets/2284.EN.ver1/da
taflow3_viewlet.html) (Jan 15, 2003)

Whale Communications, "Secure Logoff Demo"
[http://www.whalecommunications.com/site/SFunctions/Viewlets/2282.EN.ver1/w
ebmailfinal_viewlet.html](http://www.whalecommunications.com/site/SFunctions/Viewlets/2282.EN.ver1/w
ebmailfinal_viewlet.html) (Jan 15, 2003)

© SANS Institute 2003, Author retains full rights



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS London 2009	London, United Kingdom	Nov 28, 2009 - Dec 06, 2009	Live Event
SANS WhatWorks in Incident Detection Summit 2009	Washington, DC	Dec 09, 2009 - Dec 10, 2009	Live Event
SANS CDI East 2009	Washington, DC	Dec 11, 2009 - Dec 18, 2009	Live Event
SANS WhatWorks in Data Leakage Prevention and Encryption Summit 2010	New Orleans, LA	Jan 07, 2010 - Jan 12, 2010	Live Event
SANS Security East 2010	New Orleans, LA	Jan 10, 2010 - Jan 18, 2010	Live Event
SANS AppSec 2010 and WhatWorks in AppSec Summit	San Francisco, CA	Jan 29, 2010 - Feb 05, 2010	Live Event
SANS Phoenix 2010	Phoenix, AZ	Feb 14, 2010 - Feb 20, 2010	Live Event
SANS Tokyo 2010 Spring	Tokyo, Japan	Feb 15, 2010 - Feb 20, 2010	Live Event
SANS Geneva CISSP at HEG 2009 Autumn	OnlineSwitzerland	Nov 23, 2009 - Nov 28, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced