



Mitel Networks 6000 Managed Application Server Security Overview

White Paper

Release 1.2 March 2003

SME Solutions Business Unit, Mitel Networks



White Paper

Release 1.2, published March 2003. Copyright 2003 Mitel Networks Corporation

Copyright

Copyright © 2003 Mitel Networks Corporation. This document is unpublished and the foregoing notice is affixed to protect Mitel Networks Corporation in the event of inadvertent publication.

All rights reserved. No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Mitel Networks Corporation.

Trademarks

The Mitel logo and the term “i-bay” are trademarks or registered trademarks of Mitel Networks Corporation in the United States and other countries. Linux is a registered trademark of Linus Torvalds. The terms “ssh” and “Secure Shell” are trademarks of SSH Communications Security Corp. All other trademarks are the property of their respective holders.

TABLE OF CONTENTS

| | |
|--|----|
| Introduction | 1 |
| The role of the 6000 MAS..... | 2 |
| Elimination of non-essential services | 2 |
| Use of secure services | 3 |
| Open source code review..... | 3 |
| Network security | 4 |
| Stateful packet filtering | 4 |
| Disabled services do not run | 6 |
| Selective address or port binding | 6 |
| Application-level access control lists | 6 |
| Authentication and authorization mechanisms..... | 7 |
| User accounts, groups and passwords | 7 |
| Remote access | 7 |
| Secure shell (ssh)..... | 8 |
| Telnet..... | 8 |
| Point-to-point tunneling protocol (PPTP)..... | 9 |
| File transfer..... | 9 |
| File transfer protocol (FTP)..... | 10 |
| Windows networking (SMB) | 10 |
| Macintosh networking..... | 10 |
| E-mail..... | 11 |
| DNS | 11 |
| Web services | 12 |
| SSL support..... | 12 |
| CGI scripts | 13 |
| PHP | 13 |
| Webmail..... | 13 |



White Paper

| | |
|---|----|
| Web proxy server..... | 14 |
| Server console..... | 14 |
| Information bays | 14 |
| Ongoing security updates..... | 15 |
| Applications Management Center (AMC)..... | 15 |
| Server registration | 16 |
| Background to 6000 MAS/AMC communications | 16 |
| 6000 MAS/AMC synchronization..... | 17 |
| Security of the AMC..... | 17 |
| Summary | 17 |
| Conclusion | 18 |

Introduction

This white paper discusses security as it relates to the Mitel Networks 6000 Managed Application Server (MAS). It is aimed at system administrators and those with an interest in the technical aspects of system and network security.

While no network software can be 100 per cent secure, Mitel Networks has configured the 6000 MAS to provide the highest possible level of security “out of the box”. We recognize that security is important in businesses of all sizes and we want to ensure that your system and network are protected. To that end, we have taken a number of steps that, combined, produce an effective firewall solution. These steps include disabling all non-essential services, configuring services to operate in their most secure mode, providing various means of encrypted remote access and providing automatic stateful packet filtering.

Beyond these steps, we strive to automate “best practices” in Linux system administration so that tasks an expert system administrator would normally handle are performed automatically. Regardless of the administrator’s experience level, this automation relieves a great deal of the pain that is normally associated with security and system administration. It also dramatically reduces the possibility of accidental misconfiguration through human error.

This document discusses the major components of the 6000 MAS as they relate to security and the technical steps that have been taken to ensure the integrity and security of the system.

The role of the 6000 MAS

Security, reliability and ease-of-use are core attributes of the 6000 MAS. To achieve these objectives, Mitel Networks builds on the widely acknowledged reliability and flexibility of the Linux operating system, and solves the problem of complexity through a simplified installation process and web-based administration. Once installed, the 6000 MAS provides security and a rich set of Internet services including e-mail, webmail, virus protection, web hosting, web access control, secure remote access, ftp hosting, file and print sharing and many other features. The 6000 MAS software runs on standard Intel hardware, works with virtually any Internet provider, and allows customers to use their choice of desktop platform and client software.

The 6000 MAS can be configured in either of two modes of operation. In *server-only* mode, the 6000 MAS operates as a standalone server on a local network and provides file and network services to all systems on that network. In *server and gateway* mode, the 6000 MAS is configured with one network connection to the local network and a second connection to the Internet. In addition to providing file and network services to the local network, it also acts as a gateway allowing the entire local network to access the Internet.

Elimination of non-essential services

By definition, the developers of a generic operating system or software package such as Windows or Red Hat Linux cannot know exactly how that product will actually be deployed by the end user. For that reason, they generally configure the operating system so that it is capable of supporting many different types of server and workstation uses. Many services are included on the system that may not ever be used by an individual customer. This provides maximum flexibility, but also creates myriad potential system vulnerabilities. When an end user installs such a generic package, these optional services frequently open security holes into that system.

A cardinal rule of system security can be summarized as, "*Run only the absolute minimum number of services necessary for your operations*". Mitel Networks has followed this rule in developing the 6000 MAS software. Because the product has been designed to perform specific, defined tasks, we know precisely how the vast majority of users are going to use the server and what services they will require. All services not required to perform those tasks are removed from the package. Hence, unnecessary services such as NFS, NIS, the Berkeley "r" suite of programs (such as *rsh* and *rwhod*) and many others are not included with the product.

For similar reasons, the 6000 MAS does not ship with many of the packages that are included with a standard Red Hat installation. For example, the 6000 MAS does not include any of the standard compilers or development libraries (note that these development tools have been used in the past to install compromised programs during network attacks). Additionally, we have eliminated most of the user tools that would be used in a Linux workstation configuration, such as the X Window System and associated programs.

In short, if we could not identify a *need* to include a package or service in the product that would benefit customers with their daily operations, we eliminated it. This emphasis on simplicity helps to minimize security risks to the system.

Use of secure services

As part of our security review of the base Linux operating system, we also evaluate services that are included in the standard Red Hat release to determine if there are more secure alternatives. For instance, we have replaced the following services from Red Hat 7.1:

- **sendmail** - Given the number of security vulnerabilities reported in sendmail over the years, we have instead opted to use qmail and mailfront, both of which have been designed from the beginning with security in mind.
- **wu-ftpd** - Like sendmail, wu-ftpd has suffered from a history of security flaws. We chose proftpd as a replacement because of its focus on security as well as our ability to more easily configure it to limit access.

These services will be discussed in more detail in other sections of this document.

Open source code review

From a security standpoint, one of the great strengths of the Mitel Networks 6000 MAS is that the source code of the base server software (the Mitel Networks SME Server) is completely open and available to anyone to examine and review for potential security holes. At first glance, this statement might seem counter-intuitive. Why do we say that our open source process is in fact more secure than traditional “closed source” or “proprietary” development models?

The answer lies in the fact that the SME Server source code undergoes a strenuous peer review by thousands of independent developers working on the project. Given that anyone can look at our code, we benefit from a large and constantly growing developer community. For instance, more than 400 developers currently participate in the SME Server developers’ mailing list and work with the software on an ongoing basis. Many more participate in our web forums. When someone suspects a problem, that person (or someone else with the technical knowledge) can look directly at the source code and examine how we are implementing a particular item. If they see that there is an issue, they even have the option of implementing their own fix.

The value of open source peer review was dramatically illustrated in the year 2000 with the discovery that for eight years the Interbase database, a popular closed source database product, had contained a hard-coded username and password that would allow anyone knowing that user/password combination to access any Interbase database. The developers had put this “back door” in the product to solve a particular authentication problem. For eight years this security vulnerability had been there. It is impossible to know how many databases might have been compromised. How was the hole found? In mid-2000, Interbase opened its source code and made it available on the Internet. A developer in Germany was looking through the source code and found this back door. He immediately alerted the product developers, who quickly released an update and disabled the back door in new versions of the product. Had the code not been available, it is impossible to say how long this vulnerability might have persisted and how often intruders might have exploited this back door.

We believe that the fact that our code is open encourages a much stronger internal code review process than might otherwise be the case. All of our staff developers know that others will see the code, and for that reason they take steps to ensure that the code is as secure and tight as possible. Our developer community is extremely active, strong, diverse and not at all hesitant to test our code and push the edges of what we say it can and should do. We welcome that scrutiny as we firmly believe that through that process, the 6000 MAS product becomes that much more secure.

Network security

For a server functioning as a network gateway, the security related to the underlying basic network connection is of critical concern. We take this extremely seriously and use multiple tools and layers to restrict access. It starts with the fundamental distinction that in server and gateway mode, we have an internal network interface card connected to the local network and an external connection to the outside Internet, through either another network interface card or a dial-up modem. The internal card will allow most connections from the local network, but connections to the external interface are subject to extremely tight controls.

In this arrangement we use network address translation (NAT) to masquerade the entire internal network behind a single external IP address. In the recommended (and default) 6000 MAS configuration, all internal systems have non-routable private IP addresses (per RFC1918) and there is therefore no possible way for a connection to be made from the external Internet to any internal machine. This allows us to concentrate all network security resources on protecting the server and external interface.

When we speak of network security, we wish to secure the server so that all actions taken by the server in response to external network packets are defined, and all responses to external network packets are authorized and conform to a defined policy.

We achieve this restriction of server response to external network packets by means of multiple restrictive layers, described below.

Stateful packet filtering

All traffic through an IP network such as the Internet is sent in the form of packets, which consist of a header and a body. The header contains information about where the packet is going, where it came from, the type of the packet, and other administrative details. The body is the actual data being transmitted.

A packet filter is software that looks at the header of each packet and then either accepts or rejects it based on pre-defined policies. For example, the packet-filtering rules may be configured to permit incoming https connections from a particular host, but deny access from other hosts. The packet simply traverses the list of rules until it matches a pattern – one that either permits it or rejects it.

Packet filtering can be either stateless or stateful. A stateless packet filter examines each packet as a separate entity, meaning that each packet must have a rule associated with it. A stateful packet filter, in contrast, examines each packet in the context in which it is received. A stateful firewall can detect that a packet is not part of an ongoing session and can be configured to deny entry to the packet. A stateful firewall is therefore more secure than a stateless firewall because it generally requires fewer rules, reducing the risk of error or omission.

The 6000 MAS (version 5.6 or later) implements stateful packet filtering using Linux IP Tables and connection tracking. The IP Tables packet filter consists of several tables, each with a default policy and built-in chains of rules. A packet that is received via a network interface on the system goes through a sequence of steps before it is handled locally or forwarded to another host. Connection tracking strengthens the firewall by providing the ability to associate all packets of a particular connection with one another. The behavior of the firewall changes based on the information contained in the packet. If the packet contains information in the header that indicates it is part of an existing connection, and it matches a rule that states it is a permissible service, it is permitted to pass through the firewall. The firewall will open the required ports only long enough for that particular packet on an associated port to pass through. Only packets that are recognized as being part of an established connection are allowed to pass. (This also helps to thwart a would-be intruder who uses packets with modified headers that previously might have subverted a stateless packet filtering firewall.)

The general firewalling policy on the external interface of the 6000 MAS is that all incoming packets are denied except those that are explicitly allowed. Denied packets are logged but otherwise elicit no response from the server; they are simply discarded. (The standard configuration is not to log broadcast "noise" found on typical ISP networks such as Windows file-sharing and Routing Information Protocol messages, but logging of these denied packets can be configured.)

The set of explicitly allowed incoming packets is configurable. Each of the services offered by the server can be enabled or disabled in a configuration database. A subset of the services may be available as a public service. However, each of these services is optional, and can be restricted to private access (i.e. available only on the local network). Whenever this configuration database is changed, the packet filter is reconfigured to enforce the revised access policy.

It must be emphasized that each of these security layers is managed automatically. Indeed, the firewall does not even have a user interface. Instead, whenever the administrator changes the user settings, the firewall rules are updated automatically to provide the tightest possible security that enables the selected services to function. This holistic approach to security completely eliminates the most common source of network security problems – human error in configuring the firewall and server applications. Contrast this with a network environment that consists of a standalone firewall and separate computers performing such roles as web server, e-mail server, file server, etc. To enable public access to any of those services, an administrator must first configure the firewall to permit incoming requests (including e-mail) to flow from the Internet through to the server computers. This introduces complexity and opportunity for error. Even a highly trained administrator can easily overlook a small detail that would leave the network vulnerable.

The following example illustrates the benefit of this approach. One of the features of the 6000 MAS is the ability to set its clock from any one of thousands of public time servers on the Internet and to keep it synchronized over time using a protocol called NTP. With conventional networking products, the system administrator would first need to install an NTP server. He would then need to manually configure the firewall so as to enable public connections to port 123 (which is used by the ntp software) and forward them to the NTP server. If the system administrator was extremely

diligent, he would look up the IP addresses of the particular public time server he has chosen to use and manually key them in to the firewall in such a fashion as to permit public connections to port 123 only from those specific addresses. The NTP server itself could not automatically configure the firewall, since they are separate systems.

In contrast, the 6000 MAS eliminates all of this extra work and ensures that the firewall is configured with the tightest possible rule set. When the administrator enters the hostname of a public NTP server using the 6000 MAS's web interface, the 6000 MAS's firewalling code automatically looks up the IP address(es) of the NTP server and adjusts the firewalling rules to permit access only from those addresses. This recalculation is done each time a system setting is changed, thereby ensuring that ports are promptly closed when there is no longer a requirement to keep them open.

Disabled services do not run

The 6000 MAS is configured to run only services that are specifically enabled in its configuration database.

Selective address or port binding

Some applications offer the option to selectively bind to network interfaces. For services that are configured to offer access only to the internal network, this feature can be used to prevent any possibility of external connection to the network service program independent of the packet filter configuration. This feature is used, for example, in the SMB (Samba) daemon configuration.

Application-level access control lists

Each network service program is configured to provide selective service based on the IP address of the originating request. Selective service configuration is mediated by three different mechanisms:

1. By use of the TCP wrappers daemon *tcpd*, which acts as a gatekeeper application, dropping the network connection without any data transfer if the request is not from a permitted address. Accesses from permitted addresses result in the TCP wrappers daemon executing the network service program (for example, the IMAP daemon). The access restrictions are specified in the files */etc/hosts.allow* and */etc/hosts.deny*, and these files in turn are configured to comply with the policy recorded in the server configuration database.
2. By the application itself, through use of the TCP wrappers library, which is also used by the TCP wrappers daemon. The application uses the TCP wrappers library to evaluate access rules specified in */etc/hosts.allow* and */etc/hosts.deny*, and then either drops the network connection without any data transfer or provides the network service, as appropriate. An example of this class of application is *sshd*, the OpenSSH daemon, which implements the SSH protocol for secure remote access.
3. By the application itself, using application-specific access control mechanisms. A further class of applications employs its own set of mechanisms to restrict service availability according to the originating network address of the request. These applications have their own mechanism for specifying and enforcing access restrictions. Examples of this class of application are *mysql* and *squid*.

Authentication and authorization mechanisms

Once the connection has passed through all these layers, it must be authenticated by the appropriate mechanism. In most cases this involves checking that the user does in fact have a valid user account and password. In some cases, such as *pptpd* and *sshd*, encryption initialization will also occur.

User accounts, groups and passwords

Most of the services provided by the 6000 MAS are available only to users with a valid, unlocked user account. The server administrator creates user accounts through the web-based server manager. Each user account name can be up to 12 characters in length and each must be unique on the server. With an account, a user can login to receive e-mail and may also access private portions of the 6000 MAS using several file transfer methods.

Before a user can make use of his or her account, the administrator must first assign the user a password. User accounts are locked out and cannot be used until the administrator sets this initial password. Accounts without passwords are displayed in red italics in the server manager. Passwords may contain upper and lower case letters, numbers and punctuation. They are not restricted in length.

Once the initial password has been provided to the user, the user has total control over changing that password. At any time, a user can use a web browser to go to *http://servername/user-password*, enter the existing password, and then enter a new password. The administrator does not have the ability to view the user's password in any form. If the user forgets the password, the administrator cannot retrieve that password. The administrator can reset the password and communicate that new password to the user, but the administrator can never see the actual password used by the user.

User accounts, once created, can be assigned to various group accounts to simplify administration. The group can in turn be assigned specific permissions. For instance, the ability to save files in a specific directory or information bay ("i-bay") can be restricted to members of a certain group. Users can be members of multiple groups.

Note that as described in the next section, only one user, root, is configured by default to be able to login to the 6000 MAS and access the Linux shell prompt.

Remote access

In any network configuration, users typically want access to the network from remote locations. Examples may include employees who wish to work from home or who require the ability to connect while travelling. Your system administrator or Mitel Networks Solution Provider may also need to connect to your network. The challenge, of course, is to permit such access while ensuring that your system remains secure.

To meet this need, the 6000 MAS supports several forms of secure remote access. Services such as e-mail access, the web server and ftp can be configured individually to allow private access (from the local network only) or public access (from anywhere on the Internet, as with a public web site). In the case of some of those services, you may choose to allow public access but require the use of a password. These services will be discussed in more detail below.

Three services are specifically intended to allow remote login to the server (ssh and telnet) and to the network (PPTP). These will be covered in this section. It should be noted that all of these services are disabled by default. The server administrator must specifically enable them for such access to occur.

If either of the services that allow remote login to the server are enabled (ssh or telnet), by default only one account is able to login to the server. Logging in as the admin user will bring you to the 6000 MAS server console.

For ssh, the server manager also has the option to allow administrative access. While this feature is disabled by default, enabling it will allow the root user to login via ssh and access the standard Linux command prompt.

By default, no other user accounts are configured to allow a login to the server. If the administrator wishes to allow another user to login to the server remotely, he or she must first login as the root user and then change the user account shell to be `/bin/bash` using the `chsh` command. Without this change, the user will not be able to login to the server using either ssh or telnet.

Secure shell (ssh)

The secure shell (ssh) command provides a secure, encrypted method of communication between a client and server. Unlike telnet, passwords are encrypted in transit and a secure session key is used to encrypt all packets sent between the client and the server. ssh and its companion program scp (secure copy) are available for Linux/UNIX, Windows, Macintosh and other client operating systems. In its simplest form, use of ssh merely involves initiating the command and entering the user account password. The user will then see a Linux command prompt and can begin entering Linux commands.

The implementation of ssh used by the 6000 MAS is *OpenSSH*. It supports both the SSH1 and SSH2 protocols as well as both DSA and RSA authentication.

When ssh access is enabled, a user may connect and enter his or her user account password to gain access to the system. Note that there is a time delay between login prompts, making brute force attacks on good passwords impractical.

As an additional security measure when secure remote access is desired, the 6000 MAS supports ssh using RSA authentication. In this mode, an ssh key is generated on the client computer system and then added to the list of allowed keys on the server. Only users connecting from a system with an authorized key will be allowed to login to the system.

Note that all ssh access is disabled by default.

Telnet

Because telnet has traditionally been used as a tool for remote access, the 6000 MAS supports telnet access. However, it is disabled by default. The primary security problem with telnet is that it transmits all user names and passwords over the network without any form of encryption. Someone operating "packet sniffing" software and connected to any network between your 6000 MAS and the remote machine may be able to intercept and read any user names and passwords and thus could gain access to your system. For that reason we strongly discourage the use of telnet and encourage users to use ssh instead.

Within the server manager, telnet access can be restricted to the local network only or allowed from the entire network. It is possible for the “admin” user to access the server console via telnet – although, again, because of the security implications, this is strongly discouraged. Access by the “root” user to the Linux command line is not allowed through telnet.

Point-to-point tunneling protocol (PPTP)

While ssh meets many remote access needs, many users simply want to connect to their remote network and then access e-mail or use a file manager (such as Windows Explorer or Network Neighborhood) to view and access files across the network.

The 6000 MAS provides such network access using the Point-to-Point Tunneling Protocol (PPTP). PPTP allows users to establish a virtual private network between a remote client computer and the 6000 MAS and an internal network. It creates a secure encrypted channel between the client machine and the server. As far as the server is concerned, the client computer appears to be on the local internal network and can access all resources that would normally be available to the user if that user were connected to the internal LAN.

When Microsoft first introduced PPTP, many implementations suffered from poor security and the protocol gained a reputation for being insecure. Since that time, the quality of the protocol definition and its implementations have improved dramatically, to the point where PPTP now offers a reliable and highly secure connection.

PPTP clients are available for all recent versions of Microsoft Windows and are typically installed by default. Users typically launch a PPTP connection by double-clicking an icon and then entering a password.

Because PPTP allows a remote client to appear as though it is a local user, with access to anything on the local network, the security of the passwords in transit is paramount. For that reason, we require client systems to use 128-bit encryption. The 6000 MAS will not accept connections from PPTP clients that use 40-bit encryption. This may require an upgrade to the PPTP component of some of your client systems.

Like ssh and telnet, PPTP access is specifically *disabled* and must be enabled through the server manager. When enabling access, the server administrator may specify the maximum number of PPTP clients that will be permitted to access the system at any given time.

File transfer

One of the main reasons users want remote access is to be able to retrieve or use files located on the server. The 6000 MAS allows users to access files via the FTP protocol or through standard Windows and Macintosh networking.

File transfer protocol (FTP)

The 6000 MAS provides FTP access to allow users to upload or download files to and from the server. The specific FTP server included with the software is *proftpd*, configured with the latest security updates and patches.

In the default configuration, ftp access for users is allowed on the local (internal) network, but not from the external network. A user must login with a valid user name and password combination in order to access files.

Through the server manager, it is possible to configure the server to allow public (external) FTP access for users. Mitel Networks strongly discourages this action, however, because ftp, like telnet, transmits passwords from the client to the server as clear, unencrypted text. Instead, we recommend that users use the scp (secure copy) program provided with the ssh family of tools.

Anonymous ftp access is allowed on the local network for read access only. Information bays also may have a username and password associated with them and this information can be used for read access only. Under no circumstances can anonymous i-bay users upload information. The ability to write to the server is restricted to users with a valid user account on the server manager.

The rules governing FTP access to i-bays can be configured for each individual i-bay and can be configured to allow either private or public access. However, in the Remote Access panel of the server manager, the administrator has the ability to set an FTP access policy that will override all other FTP settings. The administrator also has the ability to disable public (external) FTP access or, in fact, to completely disable all FTP access from both the internal and external networks.

Windows networking (SMB)

Users may access files on the 6000 MAS using standard Windows networking through such tools as the Windows Explorer, Network Neighborhood or My Network. They may connect either to their personal (home) directory on the server or to one of the information bay directories. Connections occur through the standard Server Message Block (SMB) protocol used within Microsoft networking.

Each user's home directory is protected so that only the user may read and write to that "share". In the process of doing so, the user must enter the password for that particular user account on the server.

Shares for information bays are also visible in the browse list. Access to such shares is controlled by the configuration for each specific i-bay. An i-bay is assigned a group ownership and the default configuration limits read and write access only to group members. A user would therefore need to be a member of the appropriate group in order to access the i-bay.

The 6000 MAS uses samba to allow Windows users to access server directories via the SMB protocol.

Macintosh networking

The 6000 MAS uses an implementation of the AppleTalk file sharing protocols called netatalk to support file transfer to and from Macintosh systems. As with Windows networking, users must supply a valid username and password to access private directories on the server. Macintosh users connect to the folders using the regular Chooser within the Macintosh operating system.

E-mail

Because e-mail is mission-critical for almost all organizations, it is extremely important that the mail server component of the 6000 MAS be extremely secure. For this reason, Mitel Networks has replaced the standard Linux sendmail program with the highly secure qmail server. qmail was designed from the beginning with security in mind. The entire architecture of qmail is designed to minimize the possibilities for security exploits.

While qmail alone is extremely secure, the developers of the 6000 MAS went one step further and chose a more flexible yet secure program called mailfront for the mail server to which all SMTP mail connections (both outbound and inbound) are made. mailfront makes it possible to further restrict exactly who can send in e-mail (for use in, for instance, blocking spam) and also provides hooks that can be used for filters such as content-filtering and virus scanning.

While qmail and mailfront provide the mail server functionality, most users will be using the POP3 or IMAP protocols to read their e-mail. The 6000 MAS supports both protocols. By default, POP3/IMAP access is only available to users on the local network. If you wish to allow users to access their e-mail via POP3 or IMAP from remote systems outside your network, the server administrator must specifically enable such "Public" access through the server manager.

Note that under *no* circumstances are any users outside of the local network allowed to *send* mail to other external users through your mail server. The mail server (mailfront) will only accept mail messages from external sources that are for local users. This is designed to prevent abuse of the server by spammers as a mail relay. External users who wish to send mail to other external users must either connect to their ISP's mail server or use PPTP to establish a VPN connection to the internal side of the 6000 MAS. (In the latter case, the 6000 MAS will accept mail for other external users because the PPTP-connected user is considered to be on the local network.)

DNS

As with most Linux systems, we use the industry-standard BIND server to provide Domain Name Service (DNS) access to the local network. Because of recent security exploits related to BIND, we are constantly monitoring BIND security mailing lists and regularly update our system to the most current and secure version of the BIND program.

We take additional steps to ensure that the system is safe. For instance, the BIND daemon (called *named*) is set to run as the local user *dns* instead of the normal configuration of having *named* run as the root user. In addition to running *named* as an unprivileged user, *named* is further restricted by being forced to run in a “chrooted jail”. Essentially, this means that the program has an extremely restricted view of the system, which it thinks is in fact the entire system. In the event that somehow the *named* daemon was compromised, the attacker would not be able to see anything outside of the limited area in which the *named* daemon is confined.

Further, DNS access is only allowed from the internal local network. Users on the external Internet are not able to connect to the DNS server because it is configured to listen only on the internal network.

Web services

Web services on the 6000 MAS are provided through the open source Apache web server. As the most widely deployed web server on the Internet, Apache is subjected to continuous, extensive source code peer review and has a solid record for security. The 6000 MAS supports both standard HTTP connections as well as secure HTTPS connections that use the Secure Socket Layer (SSL) protocol.

There are actually two Apache server daemons running on the 6000 MAS. One runs on ports 80 (HTTP) and 443 (HTTPS) and provides standard user access to the primary web site, i-bays or webmail. The second operates on port 980 and provides access to the server manager. In default configuration, a user can only connect to it on the local network; in addition, the user must know the password to the admin user account.

To further secure the server, the main Apache web server runs on the 6000 MAS as the user “*www*” in a severely restricted environment. The administrative Apache server runs as the user “*admin*” which also has a restricted shell (the server console).

SSL support

As mentioned above, the primary Apache server supports SSL authentication and listens on the standard port 443 for HTTPS connections. During the installation of the software, a set of 128-bit RSA keys is generated by the *openssl* command. The public RSA key is then placed in a self-signed X.509 certificate. This certificate is presented to all browsers attempting to connect via HTTPS.

The OpenSSL Project has developed an open source, commercial-grade implementation of the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols. OpenSSL is widely used throughout the Linux and BSD UNIX world and is also used on other versions of UNIX. As is the case with the 6000 MAS, OpenSSL is often used in conjunction with the Apache web server.

CGI scripts

The execution of CGI scripts can significantly impact web server security. On the 6000 MAS, CGI scripts are disabled by default and must be specifically enabled by the server administrator for the i-bay in which the scripts are to be executed. Once enabled, CGI scripts can be executed if they are placed in the cgi-bin directory found in each information bay and in the primary directory used for the main web site. As this separate directory is not viewable by regular HTTP requests, users cannot see the contents of the actual CGI scripts.

PHP

The webmail component of the 6000 MAS makes use of the PHP scripting module for the Apache web server. PHP is a robust language that allows people to create dynamically generated content for their web sites quickly and easily. For example, a developer could create a discussion forum or a catalog that links to a database from which it extracts the actual data. PHP is similar conceptually to Microsoft's Active Server Pages (ASP) and provides similar functionality.

Users may choose to enable the use of PHP in each i-bay through the "Enable dynamic content" checkbox in the i-bay configuration screen of the server manager. PHP is disabled by default and must be specifically enabled by the server administrator.

While this allows users to easily add dynamic content to their web sites and may be a great benefit to your users, you should be aware of an inherent weakness within server-based active content such as that of PHP. With PHP enabled, a knowledgeable user could upload a PHP script to the i-bay and then call that script to read any file that the Apache userid has access to. For instance, if a user did not have access to an i-bay called "sales", but did have write access to an i-bay called "research" where PHP was enabled, the user could upload a PHP script into the research i-bay that, when called through a web browser, would open and display files found in the sales i-bay.

As this is part of PHP's basic functionality, and is also possible through the use of the CGI scripts mentioned earlier, we recommend that administrators enable dynamic content only for i-bays where write access is restricted to the administrator, or where write access is restricted to group of trusted users.

Webmail

The webmail functionality of the 6000 MAS is provided through the Internet Messaging Program (IMP) open source software package created by the Horde Project. It is disabled by default and must be specifically enabled by the server administrator before users can access the server. Once enabled, the IMP software uses PHP scripts to connect to a MySQL database that starts running on the server.

When the server administrator enables webmail, it can be set to use secure connections via Secure Socket Layer (SSL) connections (commonly referred to as "HTTPS" access) or to allow both standard HTTP and HTTPS connections. Because user account names and passwords will be transmitted across the network or Internet, we strongly recommend that webmail be enabled in the secure HTTPS mode only. This will ensure that all communication between the client web browser and the 6000 MAS is encrypted during transit.

Web proxy server

In addition to the standard Apache web server, the 6000 MAS comes configured with a fully functional proxy and caching web/ftp server known as "squid" (running on the standard port 3128). To improve performance and security, this proxy is "transparent", meaning that all outgoing web and FTP requests are automatically redirected through the proxy – regardless of how the web browser clients are configured. This makes it simple to control and audit users' web browsing activity.

In conjunction with the available Web Access Control application, the proxy server can be used to provide flexible, centralized control over local web browsing. Sites can be blocked by category, by domain, and by URL patterns. User authentication creates log files showing which users have accessed which web pages, and a simple web-based interface makes it easy to block specific recently visited sites from being revisited by anyone on the network.

Server console

The server console program is one of the means by which someone can administer the 6000 MAS. In the default configuration, the server console appears on the monitor of the server after the initial reboot during the installation process. It can also be activated by logging into the 6000 MAS locally or remotely as the user "admin". From the server console, a user can launch a text-based browser to access the server manager. Between the console and web manager, the administrator has full access to the entire 6000 MAS configuration. Note that the admin password is required to access the server manager via a browser.

If the console is set so that it displays automatically on the system, anyone with physical access to the server will be able to use the console. In situations where it is not possible to guarantee the physical security of the monitor and keyboard of the 6000 MAS, Mitel Networks recommends that the system be configured to require a login before the console can be viewed.

Information bays

Information bays, or i-bays, are areas on the server in which data can be stored and made accessible through a variety of methods. Files in an i-bay can be accessed by means of a web browser, Windows and Macintosh file sharing and/or FTP access, either public or private. While settings for i-bays have been discussed in previous sections, they can be summarized as follows:

- **Group ownership** - Each i-bay is owned by a specific group account
- **User access via file sharing and ftp** – By default, each i-bay is configured to provide read and write access only to members of the assigned group. Access can also be restricted so that only the "admin" group can write to the i-bay. Alternatively, an i-bay can be configured so that anyone can read or write to it.
- **Public access via web or anonymous ftp** - By default, this is configured for "No access". However, the server administrator can allow such access from either the local network or from the entire Internet, and can allow open access or require a password.

- **Dynamic content** - By default, this is disabled. When it is enabled, users with write access will be allowed to upload CGI or PHP scripts that can create web pages dynamically. While this is a powerful tool, administrators should be aware of the security implications described earlier.

Note that if a password is required for public access via web or anonymous ftp, the password is the one assigned to the i-bay and not to a user's regular user account. As with user accounts, the i-bay password is not set by default and users will not be able to access the i-bay until the administrator sets the password for the i-bay. Until that time, all attempts to access the i-bay will be refused.

Ongoing security updates

Mitel Networks Corporation technical staff constantly monitor industry sources of security information to be sure that no emerging issues will impact the 6000 MAS product. Because the product is based on the Red Hat Linux distribution, we pay careful attention to notices originating from Red Hat's offices or mailing lists. Each notice is carefully evaluated to determine whether there is a security impact on the 6000 MAS. Because we ship without many of the standard Linux services, many security alerts that apply to a generic Red Hat Linux installation do not apply to the 6000 MAS. Regardless, each alert is examined in detail.

We also continually monitor our web bulletin boards and our *devinfo* mailing list. The developers and administrators who use these forums are often among the first to identify potential security concerns. Many subscribe to additional security mailing lists and forward announcements and warnings from those sources.

Finally, each and every release of our product undergoes constant intensive scrutiny by our development team. As part of the release cycle, we extensively test all services and packages.

In the event that security holes are identified by our own staff or by other parties, we rapidly make fixes available through our public FTP site and our development web site and through automatic updates to registered customers.

Applications Management Center (AMC)

Every 6000 MAS must be registered with the Mitel Networks Applications Management Center (AMC) in order to receive on-line services (monitoring, virus scanning, etc.) and download applications on demand. This introduces new issues that must be understood in order to see why the overall solution is secure.

For example: What communication takes place between the server and the AMC, and how does that impact security? Does this expose the server's data to any additional security risks? Could a rogue server "hijack" a customer's on-line services? Could the AMC itself be compromised?

Server registration

To start, let us review the relationship between the server and AMC, and the communications that take place between them. Here are the steps that take place to register a new server:

1. A new service account is created on the AMC over a secure web connection, with various on-line services enabled (depending on which service package the customer has purchased).
2. After this service account is created, the customer's 6000 MAS is registered by keying in the new account number and using the registration key provided as part of the 6000 MAS software.
3. The 6000 MAS in the field then contacts the AMC over a secure connection (implemented via the SSH protocol). It uses the registration key and the new account number, and provides the AMC with a server-generated key (randomly generated, but including various details of the server's hardware configuration).
4. The AMC stores the association between this account number and the new key. The AMC generates a server-specific communication key and passes this back to the server as part of the registration process. The server must use its own specific key for all future communications now that it has passed the registration process. Further attempts to register with the same account number are detected and blocked.
5. In the event that someone changes the hardware of a server, or even makes a substantial configuration change, the server's key will change and the AMC will refuse to deliver services to that server. This is part of the overall system's security. In this situation, the service provider can perform a simple procedure through the web interfaces on the server and the AMC to erase the keys from the server and the AMC. This procedure ("resetting the signature") restores the system to the state described in step 3.

Background to 6000 MAS/AMC communications

All communications between the 6000 MAS and the AMC take place via the SSH protocol using 1024-bit keys. The 6000 MAS and the AMC can only use the registration key (provided as part of the 6000 MAS software installation) during the registration process. All future communications require the server-specific key.

All servers use a common registration key provided by the 6000 MAS software installation. In order to register, the server needs this key and a valid service account ID. Service account IDs are effectively random numbers, but there is a theoretical window of vulnerability in which any 6000 MAS could register if supplied with a valid, unregistered service account ID. This would enable that server to claim the services of the valid but currently unregistered server.

However, use of a service account ID by a "rogue" server would be detected quickly as the valid owner of the server would be unable to register. All access will be denied to the "rogue" server once the valid owner performs the signature reset described above. Further attempts by the "rogue" server to access the AMC would also be logged. Similarly, attempts to reuse existing service accounts IDs, or to move service account IDs to another computer, are logged by the AMC and access is denied.

6000 MAS/AMC synchronization

After registration, the server contacts the AMC on an hourly basis and sends a “server configuration” snapshot to the AMC (list of installed software, number of users, IP address and other parameters). In return, the server receives a “service configuration” snapshot (information about applications and services for which the customer has paid). This exchange of information is called a “SYNC” operation. It takes place securely over the SSH connection and is initiated by the server. The SYNC protocol restricts the server to specific actions on the AMC, as dictated by the services that have been subscribed for that server. It can be compared with an end-user using a web-based banking application to perform bank transactions.

The use of secure key exchange ensures that the server and AMC generate a trust relationship that cannot be circumvented by tricks such as DNS hijacking. The two-step registration process and exchange of server-generated and AMC-generated keys ensures that each end knows that it is talking to the expected host. Finally, the server initiates the SYNC connections, but the AMC is always in control and able to disable servers and services as required.

Security of the AMC

The AMC is a central point of common trust and is subject to stringent management, monitoring and release control processes. The AMC controls sensitive data such as VPN configurations, and compromise of these systems could allow VPNs to be created between unwilling parties.

The AMC is highly secure and features the same type of tight firewalling found on the 6000 MAS itself. Much of the AMC security configuration is controlled from hosts on Mitel Networks premises, ensuring a single point of control, management and auditing.

On one level, the AMC is similar to a conventional ISP or ASP in that each has the same theoretical vulnerability - a hacker who managed to break into an ISP's or ASP's systems would potentially gain access to customer data. However, in practical terms the AMC is much more secure than an ISP or an ASP since, even if a server were fooled into joining a hacker's VPN, this breach would in itself enable only limited access to the compromised server. The standard safeguards such as encrypted passwords protect the server configuration from being modified.

Summary

The design of the registration and SYNC protocols and the use of secure key exchanges and server-specific keys ensure the security of the configuration of the servers managed by the AMC. As the central point of trust, the AMC is closely monitored and managed to ensure continued service.

A separate white paper (“The Mitel Networks Applications Management Center – Architecture and Platform Software Overview”) is available for those who desire more information about the AMC and its processes.



White Paper

Conclusion

While no system can ever be completely secure, Mitel Networks 6000 Managed Application Server provides an extremely secure computing environment. Through the elimination of non-essential services, the replacement of other services with secure alternatives, and the tightening of all possible security parameters, the 6000 MAS comes “out of the box” ready to protect your network and server. Sophisticated administrators can take advantage of the product’s flexibility to address particular needs, but both they and others will continue to benefit from the 6000 MAS approach to security by default.

North America
(613) 592 2122
1 800 648 3579

**Europe, Middle-East
& Africa**
Sales: 0870 9093030
Int: +44 (0) 1291 430 000

Latin America
(613) 592 2122
1 800 648 3579

Asia-Pacific
Tel: +852 2508 9780
Fax: +852 2508 9232

www.mitel.com



THIS DOCUMENT IS PROVIDED TO YOU FOR INFORMATIONAL PURPOSES ONLY. The information furnished in this document, believed by Mitel Networks to be accurate as of the date of its publication, is subject to change without notice. Mitel Networks assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains.

M MITEL (design) is a registered trademark of Mitel Networks Corporation. All other products and services are the registered trademarks of their respective holders.

© Copyright 2003, Mitel Networks Corporation. All Rights Reserved.

GD 6441 PN 51006180, Rev. A