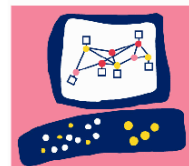


CHECK POINT™
Software Technologies Ltd.



*FireWall-1
Meta IP 4.1 UAM
Integration*

FireWall-1 Meta IP UAM Integration

Version 1.7 August 4, 1999 – Casey Tompkins

<http://www.checkpoint.com/uamintegration.htm>

Executive Summary

Network security administration has always had serious deficiencies in dynamic environments. Due to the volatile nature of address assignment in DHCP serviced networks, policy management has been limited in scope, or functionality. Either an administrator has no access to restrictions based upon user information, or users are required to authenticate against various servers as they request services.

Through the use of Meta IP 4.1's User to Address Mapper (UAM) feature, administrators can manage users through dynamically allocated addresses with a single log on. This functionality bridges the gap between MAC address resolution and full user centric policy based management in dynamic environments. The UAM works together with an authentication rule base in FireWall-1. By providing the firewall with information relating to the user identification, this integration of products enables service requests based upon a dynamic IP address to be validated within the FireWall-1 security policy at the user level.

This document will describe the configurations required for installation, as well as technical workflow diagrams that illustrate the interaction between the various components of the Meta IP 4.1 UAM and the FireWall-1 integration



This document assumes that you have a good working knowledge of FireWall-1 and Meta IP. If you are not familiar with these products please see the relevant manuals and white papers prior to proceeding with this integration.



This document assumes that Meta IP UAM/UAT Services have already been installed and are functioning properly. To verify UAM/UAT functionality, launch the Meta IP Admin Console. Select the DHCP Service or Lease Pool in question. Right-click and select Manage Leases from the menu. In the Manage Leases window, change the View to "All Leases from UAM". User log on information should be displayed with the leases.

In This Document:

<i>Executive Summary</i>	<i>page 1</i>
<i>Review: Meta IP UAM UAT</i>	<i>page 2</i>
<i>Section 1: FireWall-1 Version 4.1</i>	<i>page 4</i>
<i>FireWall-1 Version 4.1 Platform Requirements</i>	<i>page 4</i>
<i>FireWall-1 Version 4.1 UAM Installation Instructions</i>	<i>page 4</i>
<i>FireWall-1 Version 4.1 Policy Configuration</i>	<i>page 4</i>
<i>Section 2: FireWall-1 Version 4.0 SP3</i>	<i>page 6</i>
<i>FireWall-1 Version 4.0 SP3 Platform Requirements</i>	<i>page 6</i>
<i>FireWall-1 Version 4.0 SP3 Configuration (Win NT)</i>	<i>page 6</i>
<i>FireWall-1 Version 4.0 SP3 Configuration (Solaris)</i>	<i>page 8</i>
<i>FireWall-1 Version 4.0 SP3 Policy Configuration</i>	<i>page 8</i>
<i>Example</i>	<i>page 10</i>
<i>Work Flow Diagrams</i>	<i>page 11</i>
<i>Appendix A: UAM Specific files and registry changes FireWall-1 Version 4.1</i>	<i>page 12</i>
<i>Appendix B: Troubleshooting</i>	<i>page 13</i>
<i>Glossary</i>	<i>page 14</i>



Due to the improvements in the automation of the FireWall-1 UAM integration, it is highly recommended that you upgrade your FireWall-1 service to version 4.1.

Review: Meta IP UAM, UAT (NT), and MIUAT (Novell)

Meta IP integrates three services that greatly enhance the ability to monitor and control dynamically allocated networks on a per-user basis: the UAT, the UAM and the MIUAT. The User to Address Mapper service (UAM) and the User Authentication Trap daemon (UAT) work together to organize and host dynamic user information for Meta IP and 3rd party services for users on Windows NT based systems. Similarly the UAM and the Meta IP User Authentication Trap NetWare Loadable Module (MIUAT or MIUAT.NLM) work together to organize and host dynamic user information for Meta IP and 3rd party services for users logging into Novell servers.

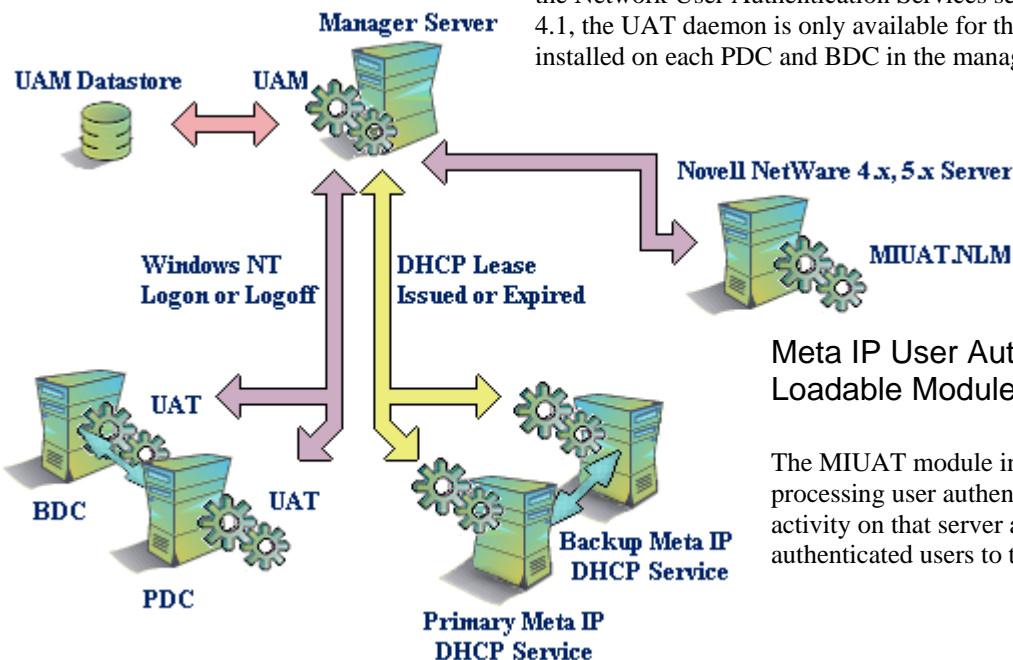
User to Address Mapper (UAM)

The UAM compiles host information from the active DHCP service, MIUAT.NLM, and the UAT. The UAM collects the MAC address, IP address, user name, and other pertinent details about each lease allocation or log on/log off. The UAM presents network managers a simple, integrated way to expand policy management to the user level without requiring permanent addresses or multiple user log ons. The UAM collates and gathers information and makes it available to other applications and services via a UDP interface. The UDP interface permits external applications to query and browse for user and workstation relationships. External applications and services may subscribe to “notifications” of User Authentication, DHCP leases and user/workstation match activities without needing to poll the UAM. This service and information availability allows for the development of user and user location aware services and applications for services such as IP Phone, user based policy enforcement, and infrastructure provisioning. The first major implementation of this is now available from the market leading FireWall-1 from Check Point Software Technologies. Integrating FireWall-1 with UAM makes it possible to apply specific rule based policies to individual users or any defined user group.

User Address Trap (UAT)

The Meta IP UAT daemon installs into the User Authentication service of a network. It monitors the log on/log off activity on that service and reports the activity to the UAM service. The UAT reports the name and host workstation information of the user to the UAM, where it can be collated with the information collected and stored from the Meta IP DHCP services. The UAT daemon is platform-specific and connects itself to the appropriate User Authentication logging system.

The design of the UAT daemon system permits the installation of the daemon only on the Network User Authentication Services servers. With the current release of Meta IP 4.1, the UAT daemon is only available for the Windows NT environment, and must be installed on each PDC and BDC in the managed network.



Meta IP User Authentication Trap NetWare Loadable Module (MIUAT.NLM)

The MIUAT module installs on each Novell server that will be processing user authentications. It monitors the log on/log off activity on that server and reports the log on/log off of authenticated users to the UAM service.

UAM Datastore

The Meta IP system, through the integration of the UAM, UAT, and DHCP services, provides a tunable method for tracking the usage of IP address leases and the users associated with them. The UAM Datastore is exported from the UAM as a .mdb file. A network administrator can also manage the date range of records retained in the UAM Datastore, allowing for full control of the UAM auditing functions, based on the needs of a particular IP network.

Section 1: FireWall-1 Version 4.1

FireWall-1 Version 4.1 Platform Requirements

- Check Point FireWall-1 Version 4.1 on Windows NT SP3 or SP4, Solaris SPARC 2.6, with a minimum 64 megabytes of RAM.
- Meta IP Version 4.1 SP2 (Build 4704) Manager Service installed on Windows NT 4.0 SP3 or SP4 with UAM/UAT functionality. Meta IP Version 4.1 DHCP Service installed on Windows NT SP3 or SP4, Solaris SPARC 2.6, HP-UX 10.20, or Linux 2.0.34 kernel with RPM install package



Always backup your systems before making any changes. This document assumes that you have a thorough backup.

FireWall-1 Version 4.1 File Requirements

- All required files for this integration are included in the FireWall-1 Version 4.1 CD, and FireWall-1 Version 4.1 download. The installation of these files is handled by the FW-1 installation. If a system does not have the required files installed, reference appendix A for assistance with locating and copying these files.

FireWall-1 Version 4.1 UAM Integration Installation

The FireWall-1 Version 4.1 installation asks the administrator if they plan to use the Meta IP UAM integration. When this option is selected, 3 UAM specific files are installed from the FireWall-1 CD and a configuration executable is processed (on Windows NT installations) to install the necessary registry changes. If FireWall-1 is installed without this additional module, you will need to add it by hand. See Appendix A on page 10 for the manual instructions.



If you are using a UAM PassPhrase that is not blank you will need to configure this value manually in the registry of your FireWall-1 host machine.

FireWall-1 Version 4.1 UAM Integration Policy Configuration

Initially users and groups must be created through the **User Manager** dialog. Click **New**, and then click **Default**. This allows you to create a generic or specific user. If you simply want to test any Windows NT authorized user use the name **generic***. Please note that generic* references any user that is not defined in the FireWall-1 user database. For a specific user, enter their Windows NT domain username (this is case sensitive; enter the name in ALL CAPS, note this is settable in FireWall 4.1 (see appendix A).

Because FireWall-1 will communicate with the MetaIP UAM service, it is necessary to establish permissions for these packets. Do this by installing the following rule:

Source	Destination	Service	Action	Track	Install On	Time
FireWall_Host MetaIP_Host	FireWall_Host MetaIP_Host	UDP Port 5004	Accept	(any)	FireWall_Host	(any)

To establish single sign-on, FireWall-1 integration with the UAM, the FireWall-1 installation needs one of the following Client Authentication rules installed:

Source	Destination	Service	Action	Track	Install On	Time
Specific_Group@any	(any)	Specific Services	Client Auth (SSO)	(any)	(any)	(any)
All Users@any	(any)	Specific Services	Client Auth (SSO)	(any)	(any)	(any)

Source can be any group or all defined users as required by the installation.

Destination can be any destination or specific resources.

Service must be a specific service or services to be monitored.

Action must be **Client Auth** with **SSO** enabled.

Track can be set to whatever is required.

Install On can be specific or **Gateways** as required by the installation.

Time can be set to whatever is required.



These rules must be above the firewall stealth rule if one exists.



If you have source client which are not UAM authenticated (i.e. statically assigned, non-DHCP, IP addresses) the rules for these clients must come before the SSO rules if they are for the same services. For example the FTP rule for allowing your static clients access must come before the FTP Single Sign On - Client Auth UAM authentication rule.

The Client Authentication action needs to be configured. To do this, right-click the **Client Auth** icon and choose **Edit Properties**. The property **Sign on Method** must be set to **Single Sign On (SSO)**. If this option does not appear verify the version of FireWall-1 and the service pack installed.

The FireWall-1 UAM integration can be customized to meet the security needs of your organization on a per-policy basis through the **Limits** tab of the **Client Auth** action. The default setting for the UAM authentication is 30 minutes, after which time communication from the user's IP address will be revalidated with the UAM. Selecting the **Refreshable Timeout** option will cause the UAM authentication to eliminate caching and users will be authenticated on every access attempt. Set this to your desired timeout, or choose **Refreshable Timeout**. The option for **Sessions Allowed** defines the number of connections the user is allowed.



Setting the Refreshable Timeout to 0 or the Sessions Allowed to 0 will cause the firewall to refuse all UAM authentication sessions.

Section 2: FireWall-1 Version 4.0 SP3

FireWall-1 Version 4.0 SP3 Platform Requirements

- Check Point FireWall-1 4.0 SP3, Solaris SPARC 2.6 or Windows NT Server 4.0 SP3 or SP4 with a minimum of 64 megabytes of RAM
- Meta IP Version 4.1 SP2 (Build 4704) Manager with UAM/UAT installed on Windows NT Server 4.0 SP3 or SP4.
- Meta IP DHCP Service installed on Windows NT Server 4.0 SP3 or SP4, Solaris 2.6 SPARC, HP-UX 10.20, or Linux 2.0.34 (RPM based).



Always backup your systems as appropriate before making any changes. This document assumes that you have a thorough backup before beginning.

FireWall-1 Version 4.0 SP3 File Requirements

All required files for this integration are available for download at <http://www.checkpoint.com/uamintegration.htm>.

The required files are as follows:

- formats.def** for all FW-1 installations.
- fwuam.dll** for Windows NT FW-1 installations.
- fwuam.so** for Solaris SPARC FW-1 installations.
- uamlib.conf** for Solaris SPARC FW-1 installations.

Windows NT Configuration Settings



THESE INSTRUCTIONS ARE **ONLY** FOR FIREWALL-1 4.0 SP3 (BUILD 4064 OR LATER)

Since it is possible to have the FireWall-1 Management Server and Packet Filtering Module (PFM) on different systems, each point will indicate which systems the step applies to. If the Management Server and the PFM are both on the same system, all of the steps apply to that single system.

MGR = Management Server

PFM = Packet Filtering Module

BOTH = Both Management Server and Packet Filtering Module

- **BOTH.** Issue an **fwstop** to stop FireWall-1.
- **BOTH.** The file `%FWDIR%\lib\setup.C` needs to be edited. Modify the file by adding the line **:has_sso (true)**. This can be done at the top section of the file *after* the open parenthesis.
- **MGR.** The `%FWDIR%\lib\fwui_head.def` file needs to be edited. Modify the file by uncommenting the line `///define HAS_SSO 1` to look like `#define HAS_SSO 1`.
- **MGR.** The file `%FWDIR%\conf\objects.C` needs to be edited. Modify the file by adding the line **:sso_resolve_src (true)**. This must be added to the file immediately following the line that includes **:props (.**
- **MGR.** Rename the `%FWDIR%\conf\objects.C.bak` file to `%FWDIR%\conf\objects.C.bak-orig`.
- **MGR.** The file `%FWDIR%\lib\formats.def` needs to be *replaced* with the new file. See the FireWall-1 CD or download the file from <http://www.checkpoint.com/uamintegration.htm>

- **BOTH.** The file `c:\winnt\system32\fwuam.dll` needs to be installed. See the See the FireWall-1 CD or download the file from <http://www.checkpoint.com/uamintegration.htm>
- **BOTH.** Windows NT Server Registry Configuration Settings. Several keys in the registry *on the firewall* need to be added or configured for the proper operation of the integration between the UAM and FIREWALL-1. Use `regedt32.exe` to modify these values. If a registry entry or hive does not currently exist, create it. The registry configuration that will be edited (or created) is located in the registry hive: `HKEY_LOCAL_MACHINE\SOFTWARE\MetaInfo\MetaIP\`

Under this hive is a list of UAM servers. This hive may already be populated if other Meta IP services are running on this machine. NOTE: Meta IP should not be running on the firewall.

`HKEY_LOCAL_MACHINE\SOFTWARE\MetaInfo\MetaIP\MI-UAT\Addresses\IP-Address\`

for example, `HKEY_LOCAL_MACHINE\SOFTWARE\MetaInfo\MetaIP\MI-UAT\Addresses\192.168.1.1`

Where the *IP-Address* hive is the IP address of the UAM server, which is the same machine running the Meta IP Management Server. Under this *IP-Address* hive, create the keys with the following values:

Key	Data Type	Value
Endpoint	REG_DWORD	hex:0x138c dec:5004
PassPhrase	REG_SZ	blank

These values assume a default installation. The **Endpoint** value is the port the UAM server is set to listen on (port 5004 decimal), and the **PassPhrase** value is blank. These settings need to match the settings in the registry on the Meta IP Manager (UAM) server. To verify that these settings are correct, look at the corresponding registry entry for **PassPhrase** on the Meta IP Manager (UAM) server in:

`HKEY_LOCAL_MACHINE\SOFTWARE\MetaInfo\MetaIP\MI-UAM\`

and the registry entry for **Endpoint** in the **MI-UAM** value:

`HKEY_LOCAL_MACHINE\SOFTWARE\MetaInfo\MetaIP\Ports\MI-UAM (REG_DWORD)`

Next, because there may be multiple UAM servers on your network, the `fwuam.dll` library needs to know which one to query. This is needed even if there is only one server defined in the registry.

This registry value must be created in:

`HKEY_LOCAL_MACHINE\SOFTWARE\MetaInfo\MetaIP\MI-UAT\Addresses\`

and should be created as follows:

Key	Data Type	Value
fwuam	REG_SZ	<i>IP-Address</i>

where *IP-Address* is the IP address of the UAM server and *MUST* match a server listed under the **Address** hive documented above.

- **BOTH.** Reboot the Management Server then the PFM to make the changes take effect. Make sure the Management Server is fully up before rebooting the PFM.

Solaris SPARC Configuration Settings



THESE INSTRUCTIONS ARE ONLY FOR FIREWALL-1 4.0 SP3 (BUILD 4064 OR LATER)

Since it is possible to have the FireWall-1 Management Server and Packet Filtering Module (PFM) on different systems, each point will indicate which systems the step applies to. If the Management Server and the PFM are both on the same system, all of the steps apply to that single system.

MGR = Management Server

PFM = Packet Filtering Module

BOTH = Both Management Server and Packet Filtering Module

- **BOTH.** Issue a **fwstop** to stop FireWall-1.
- **BOTH.** The **\$FWDIR/lib/setup.C** file needs to be edited. Modify the file by adding the line **:has_sso (true)** to the top section of the file *after* the open parenthesis.
- **MGR.** The **\$FWDIR/lib/fwui_head.def** file needs to be edited. Modify the file by uncommenting the line **##define HAS_SSO 1** to look like **#define HAS_SSO 1**.
- **MGR.** The **\$FWDIR/conf/objects.C** file needs to be edited. Modify the file by adding the line **:sso_resolve_src (true)**. This must be added immediately following the line **:props (**.
- **MGR.** Rename the **\$FWDIR/conf/objects.C.bak** file to **\$FWDIR/conf/objects.C.bak-orig**.
- **MGR.** The **\$FWDIR/lib/formats.def** file needs to be *replaced* with a new file (see the FireWall-1 CD or download the file from <http://www.checkpoint.com/uamintegration.htm>). Set the permissions and ownership of this file to match those of the FireWall-1 executable.
- **BOTH.** The file **fwuam.so** needs to be installed in **/usr/lib** from the (see the FireWall-1 CD or download the file from <http://www.checkpoint.com/uamintegration.htm>). Set the permissions and ownership of this file and directory to match those of the FireWall-1 executable.
- **BOTH. uamlib.conf** Settings: Unlike Windows NT installations of FireWall-1, there are no registry settings in Solaris, even though the Meta IP UAM is running under Windows. Under Solaris complete the following tasks instead:
 1. Create the directory **/etc/metaip/**.
 2. Copy the **uamlib.conf** file (See the FireWall-1 CD or download the file from www.checkpoint.com) to this new directory **/etc/metaip/**.
 3. Change the ownership and permissions on the **uamlib.conf** file and directory to match those of the firewall executable.
 4. Once the **uamlib.conf** file is relocated, edit this text file by replacing both instances of **<UAM HOST IP ADDRESS>** with the IP address of the Meta IP UAM Management Server. NOTE: This server will have **Meta IP/User Address Mapper 4.1** listed in NT Services. (See the FireWall-1 CD or download the file from <http://www.checkpoint.com/uamintegration.htm>)
- **BOTH.** Reboot the Management Server then the PFM to make the changes take effect. Make sure the Management Server is fully up before rebooting the PFM.

FireWall-1 Version 4.0 SP3 Security Policy Configuration

Initially users and groups must be created. To do this enter the **User Manager** Dialog. Click **New, Default**. This allows you to create a generic or specific user. If you simply want to test any Windows NT authorized user use the name **generic***. Please note that generic* references any user not defined in the FIREWALL-1 user database. For a specific user enter their Windows NT domain username (this is case sensitive, enter the name in ALL CAPS).

Since the FireWall-1 host will be communicating with the MetaIP UAM service it is necessary to establish permissions for these packets. Do this by installing the following rule:

Source	Destination	Service	Action	Track	Install On	Time
FireWall_Host MetaIP_Host	FireWall_Host MetaIP_Host	UDP Port 5004	Accept	(any)	FireWall_Host	Unrestricted

To establish single sign-on FireWall-1 integration with the UAM the FireWall-1 installation needs one of the following Client Authentication rules installed:

Source	Destination	Service	Action	Track	Install On	Time
Specific_Group@any	Specific Destination	Specific Services	Client Auth (SSO)	(any)	Specific	(any)
All users@any	Any	Specific Services	Client Auth (SSO)	(any)	Generic	(any)

Source can be any group or all defined users as required by the installation.

Destination can be any destination or specific resources.

Service must be a specific service or services to be monitored.

Action must be **Client Auth** with **SSO** enabled.

Track can be set to whatever is required.

Install On can be specific or **Gateways** as required by the installation.

Time can be set to whatever is required.



These rules must be above the firewall stealth rule if one exists.



If you have source clients which are not UAM authenticated (i.e. statically assigned, non-DHCP, IP addresses) the rules for these clients must come before the SSO rules if they are for the same services. For example the FTP rule for allowing your static clients access must come before the FTP Single Sign On - Client Auth UAM authentication rule.

The Client Authentication action needs to be configured. To do this right-click the Client Auth icon. Choose Edit Properties. The property Sign on Method must be set to Single Sign On (SSO). If this option does not appear verify the version of FIREWALL-1 and the service pack installed.

Example

At this point the configurations are complete. Reinstall the security policy, then stop and restart the Check Point FireWall-1 service. Below is an example of several users attempting to use the service FTP through the FireWall-1 product (4.0 SP3 on Windows NT) with this Client Authentication rule:

Source	Destination	Service	Action	Track	Install On	Time
All users@any	Any	FTP	Client Auth	Long	Concrete (the FireWall-1 host)	Any

Note: The following users have been added in the **User Manager** Dialog.

JACKSONV
GABRIELLAV
BENJAMINH

The following user was not added in the User Manager Dialog.

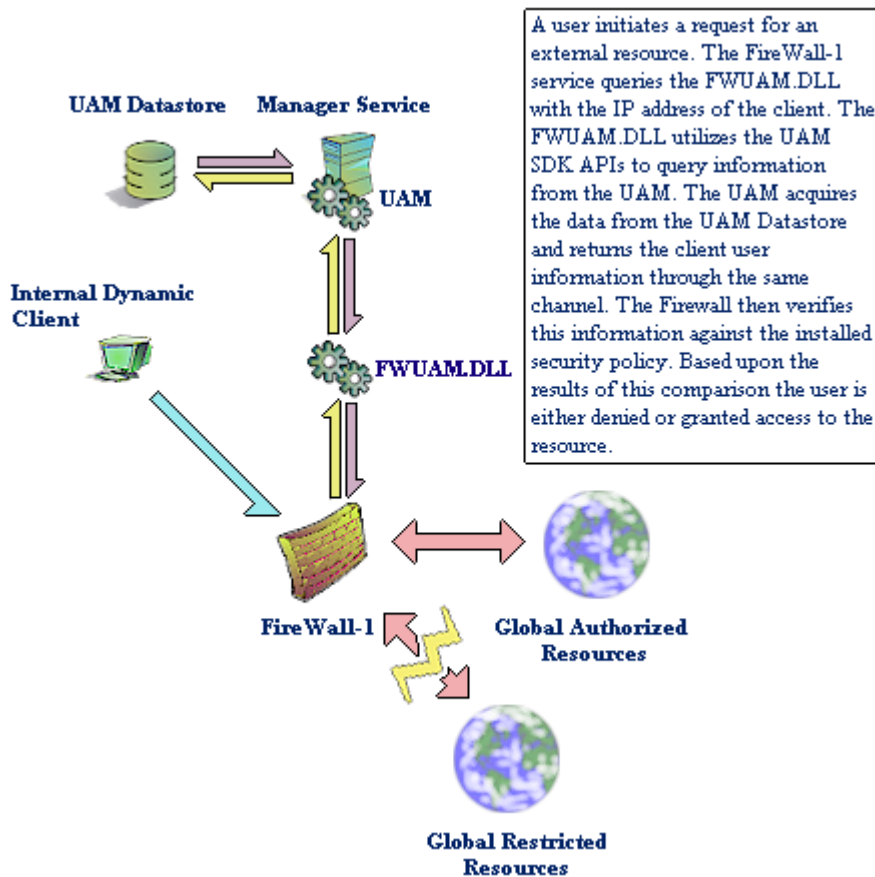
JOEHACKER

Date	Time	Type	Action	Service	User	Info.
26Jan1999	9:48:56	log	authorize	ftp	JACKSONV	reason SSO Authorization(Package:MetaIP UAMUJAT)
26Jan1999	9:48:56	log	accept	ftp	JACKSONV	srcname SEATTLE.metademo.com
26Jan1999	9:49:42	log	accept	ftp	JACKSONV	srcname SEATTLE.metademo.com
26Jan1999	9:49:42	log	accept	ftp	JACKSONV	srcname SEATTLE.metademo.com
26Jan1999	9:50:19	log	accept	ftp	JACKSONV	srcname SEATTLE.metademo.com
26Jan1999	9:50:19	log	accept	ftp	JACKSONV	srcname SEATTLE.metademo.com
26Jan1999	9:51:26	alert	reject	ftp	JOEHACKER	reason Unknown User(Package:MetaIP UAMUJAT)
26Jan1999	9:53:49	log	authorize	ftp	GABRIELLAV	reason SSO Authorization(Package:MetaIP UAMUJAT)
26Jan1999	9:53:49	log	accept	ftp	GABRIELLAV	srcname PULMAN.metademo.com
26Jan1999	9:53:49	log	accept	ftp	GABRIELLAV	srcname PULMAN.metademo.com
26Jan1999	9:54:52	log	accept	ftp	GABRIELLAV	srcname PULMAN.metademo.com
26Jan1999	9:54:52	log	accept	ftp	GABRIELLAV	srcname PULMAN.metademo.com
26Jan1999	9:55:52	log	accept	ftp	GABRIELLAV	srcname PULMAN.metademo.com
26Jan1999	9:55:52	log	authorize	ftp	BENJAMINH	reason SSO Authorization(Package:MetaIP UAMUJAT)
26Jan1999	9:55:52	log	accept	ftp	BENJAMINH	srcname TACOMA.metademo.com

Workflow Diagrams

The Meta IP 4.1 and Check Point FireWall-1 Integration Workflow

Meta IP 4.1 includes a revolutionary new service that enables policy based management at the user level in dynamic environments with a single sign on. The recently announced integration with Check Point FireWall-1 is the first implementation of this. Through the configuration of the policy rule base to include client authentication at the user or user group level, and the implementation of the UAM/UAT services of the Meta IP system, a network administrator is able to specifically set permissions on individuals regardless of their location or address.



Appendix A: UAM Specific files and registry changes under FireWall-1 Version 4.1



THIS INFORMATION IS ONLY FOR FireWall-1 4.1

This appendix provides a listing of the UAM specific files and registry changes that are managed by the FireWall-1 installation. Please note that this is for reference only as this integration work is automated through the installation of FireWall-1 Version 4.1.



These are the steps to complete if the FireWall was initially installed without Meta IP UAM integration.

The following files are installed from the FIREWALL-1 CD under Windows NT:

c:\winnt\system32\uamlib.dll
c:\winnt\system32\fwuam.dll
c:\winnt\system32\msvcp50.dll

The following files are installed from the FIREWALL-1 CD under Solaris:

/usr/lib/fwuam.so
/etc/metaip/uamlib.conf

Each of these file's permissions are changed to the ownership and permissions of the firewall executable. Also the **/etc/metaip/** directory must be given executable permission.

The **uamlib.conf** file is edited by replacing both instances of **<UAM HOST IP ADDRESS>** with the IP address of the server running the Meta IP User to Address Mapper service.

The following registry keys are created by the FireWall-1 installation under Windows NT:

HKEY_LOCAL_MACHINE\SOFTWARE\MetaInfo\MetaIP\MI-UAT\Addresses\<IP-address>

Key	Data Type	Value
Endpoint	REG_DWORD	hex:0x138c dec:5004
PassPhrase	REG_SZ	blank

HKEY_LOCAL_MACHINE\SOFTWARE\MetaInfo\MetaIP\MI-UAT\Addresses

Key	Data Type	Value
fwuam	REG_SZ	IP address entered in dialog



The configuration tool FWUAM.EXE on the FireWall-1 CD will create these keys and values. This can be run at any time after the FireWall-1 installation, and is automatically spawned during the initial installation.



FWUAM.EXE will not overwrite existing values if the keys already exist.



If you are using a UAM PassPhrase that is not blank you will need to configure this value manually in the registry of your FireWall-1 host machine.

Appendix B: Troubleshooting

These are common items, issues, or questions that are asked during setup.

Note that these issues are mostly apparent in FireWall-1 4.0 SP3 installations. It is recommended that administrators upgrade to FireWall-1 4.1.

- Watch for spacing in the edited files. Keep spacing consistent with the rest of the file. Certain text editors can wrap text in the saved edited files. This will be apparent by immediate failure of the FireWall-1 service.
- If the FireWall-1 service fails after a few authentications use the command `fw ver` to determine the installed version of the FireWall-1 service. Verify that the build number is at least 4064.
- The **generic*** user cannot be mixed with a group of real users in FireWall 4.0. This can be done in FireWall-1 4.1.
- User names must be in **ALL CAPS**. FireWall-1 4.1 is no longer case sensitive if the line `:clauth_tolower_users (true)` is added to the `objects.C` file.
- User names must be in the FireWall-1 user database for authentication.
- For **OS Password** authentication with **SSO**, user accounts do not need to be created on the local firewall operating system (but do need to be created in the FireWall-1 user database).
- Groups of users are done with FireWall-1 user group objects.
- The rule in the rule base must have a group of users in the **Source** column.
- The rule in the rule base must have **Client Auth** with **SSO** enabled in the **Action** column.
- For testing purposes, put the UAM rules at the top of the rule base.
- Be sure to install the **formats.def** and OS specific libraries from the FireWall CD or from the Check Point web site (Do not do this for FireWall-1 4.1)
- Double-check the Windows NT registry settings. All information must be created/entered precisely for proper functioning.
- Verify UAM functionality. From the Meta IP Admin Console, select **Manage Leases** on the DHCP service or the lease pool in question. Select from the View menu **All Leases from UAM**. If the user name does not show up in the list, the UAM database does not have the information. Do a DHCP **release** then **renew** and **log out** then **log in** to the NT Domain on the Client System. If the user still does not show up, Meta IP/UAM needs to be reconfigured correctly.
- In **Client Auth** properties, it does not matter if **Source** is set to **interact with user database** or **ignore user database**.
- When editing **objects.C**, sometimes the added line will be removed. If this happens, stop the firewall and add the line to both **\$FWDIR/conf/objects.C** and **\$FWDIR/database/objects.C**. Start the firewall and reinstall the policy. (Do not edit this file under FireWall-1 4.1—all file editing is automatic).
- If the UAM rule in the rule base seems to be getting skipped (as seen from the Log Viewer), double-check the rule matching criteria. FireWall-1 will match SSO Client Auth rules according to Source, Destination, and Authenticated (Service group). From there it will act according to the rest of the matched rule. Since the UAM rule requires a user group, FireWall-1 will try and match a user from that group. If that user is not found, matching criteria will not be met for that rule and the next rule will be checked.
- If the firewall is still failing, check to verify that `fwuam.dll` or `fwuam.so` has the permissions and ownership to match those of the FireWall-1 executable.
- Re-Verify the version number of your FireWall-1 and Meta IP operating system.
- Clients not using Meta IP DHCP will fail on UAM SSO authentication rules.

Glossary

DHCP

[Dynamic Host Configuration Protocol]

DHCP provides an automated mechanism to control the allocation of IP addresses and IP network configuration data to network IP clients. The DHCP system provides for the ability to create pools of IP addresses and configuration data oriented around IP subnets. These pools can reflect physical design and or logical design of an IP network. In the Meta IP system The DHCP protocol is used by:

- The DHCP Service – the host system for this protocol in the Meta IP system
- The RADIUS Service – uses DHCP to provide IP configuration data to RADIUS clients.

UAM

[User to Address Mapper]

The UAM tracks and collates the information from Dynamic IP address allocation, and user network authentication. By combining this data in an open format other applications are able to access the data for network monitoring and policy based management at the user level in dynamic environments.

UAT

[User Authentication Trap]

The UAT is a daemon that is installed at the network authentication sites. In a Windows NT environment, this includes the PDCs as well as the BDCs. Through this daemon, the UAM is informed of all network authentications and terminations.

Copyright © 1999 Check Point Software Technologies Ltd.

All Rights Reserved

"Check Point", "Meta IP", "User Address Mapper", "User Address Trap", "Intelligent Network Protocol", "Service Management Control Protocol" are trademarks of Check Point Software Technologies Ltd. All other trademarks are the property of their respective companies. Technical information in this document is subject to change without notice.

Company Private

This document cannot be reproduced or distributed without the express prior written permission of Check Point Software Technologies Ltd.