Assisted Remediation Tool (ART) Guide

An guide to using the Assisted Remediation Tool to aid in the deployment of Assisted Remediation with DIR.

Introduction

Assisted Remediation (AR) is designed to enable end-user notification that a quarantine action has been taken on their session. HTTP redirection can be implemented to facilitate this end-user notification by returning a web page from a Remediation Web Server that informs the end system of its quarantined state. This situation is highly applicable in the deployment of the Enterasys Secure Networks Solutions, such as Dynamic Intrusion Response (DIR) and Trusted End System (TES), where an end system may be automatically quarantined as a security threat on the network. In order to aid in the deployment of Assisted Remediation on an existing enterprise network, the *Assisted Remediation Tool* (ART) was created as a configuration wizard for implementing Assisted Remediation. The first release of this tool covers the configuration of Assisted Remediation with DIR. By using ART, a network administrator is provided with a complete configuration guide to implementing Assisted Remediation on an existing network avoiding the configuration complexity of Assisted Remediation deployment.

Note that it is assumed that the users of this tool understand the premise of Assisted Remediation, as well as the implementation details of each configuration approach. To obtain background information on Assisted Remediation, please reference the following link; **http://www.enterasys.com/support/newsletter**. ART is available for download at the following link; **http://www.enterasys.com/support/tools.html**

Overview

When deploying Assisted Remediation with DIR, it is important to note that the redirection of HTTP traffic from quarantined end systems may be implemented using different approaches. The choice of approach is directly dependant on the existing support on the network infrastructure with specific technologies, such as ToS-rewrite, Policy Based Routing (PBR), and Port Web Authentication (PWA). Furthermore, each of these approaches is characterized by different implementations considerations such as security, configuration complexity, and topological restrictions. All of these factors must be taken into account before choosing an Assisted Remediation approach for deployment on the enterprise network. After the decision is made, the infrastructure devices may be configured in the deployment of Assisted Remediation.

ART is composed on two sections where a user is first aided in the selection of an Assisted Remediation approach and then assisted in its configuration. The first section, *Assisted Remediation Approach Selection*, asks the user questions about existing technology support and configuration of the infrastructure devices to determine which Assisted Remediation approaches are deployable on the network. The second section, *Assisted Remediation Approach Configuration*, begins with the user selecting the Assisted Remediation approach(es) for deployment and then walks through the complete configuration of Assisted Remediation for DIR based on a selected approach(es). The remainder of this article explains these sections of ART.

Assisted Remediation Approach Selection

The introductory window of ART, as shown in Figure 1, briefly describes the tool's objective and provides the user with two options; *Skip* or *Next*. The *Next* button begins the first section of ART, *AR Approach Selection*, while the *Skip* button moves immediately into the second section, *AR Approach Configuration*, where the user can choose the Assisted Remediation approach for deployment and immediately begin the configuration. Note that a link to a document is also presented in the introductory window for obtaining additional background information on Assisted Remediation.

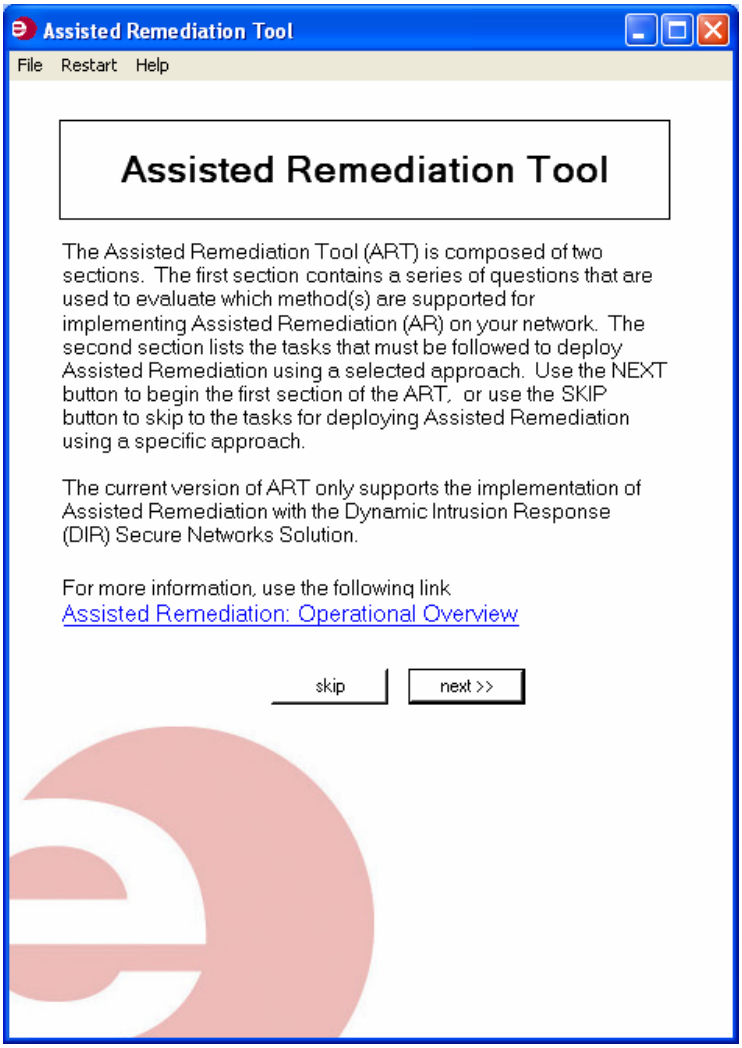

Figure 1. ART introductory window

After clicking on *Next*, a series of "yes/no" questions are posed to determine which Assisted Remediation approach(es) is supported on the existing network based on its current configuration. Figure 2 shows an example of these questions. The series of questions follows a line of reasoning that determines which Assisted Remediation approaches may be selected for configuration on the enterprise. Note that it may be necessary to implement multiple approaches to Assisted Remediation because of varied technology support and configuration across devices in the network. Therefore, these questions have been architected to evaluate the possibility of using multiple Assisted Remediation approaches for configuration concurrently on the network.

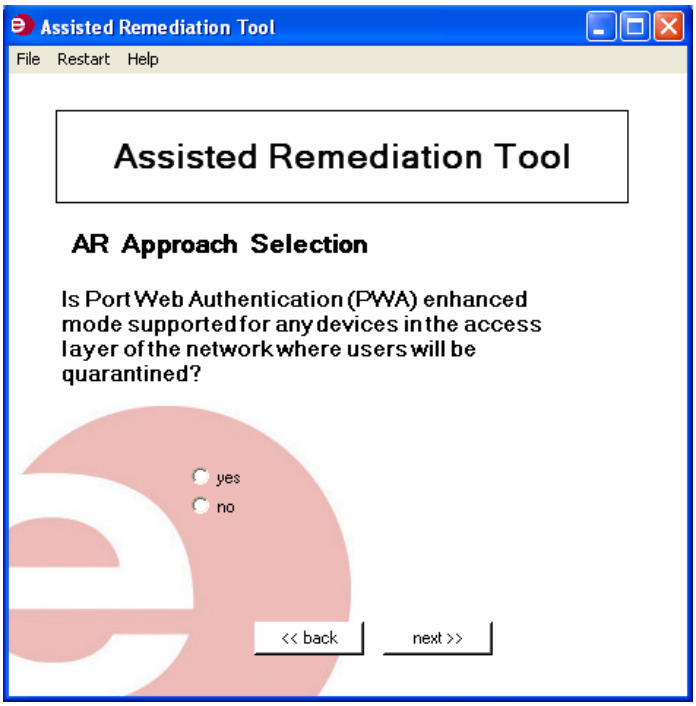

Figure 2. AR approach selection questioning

Assisted Remediation Approach Configuration

After the "yes/no" questions are completed, a window is displayed that shows all of the Assisted Remediation approaches with an indication of the approach(es) that are supported on the network, as shown in Figure 3. There exists three approaches; PWA, ToS-based PBR, or SIP-based PBR. The following briefly explains the implementation of each approach:

- The PWA approach uses NetSight ASM with custom scripting and the HTTP traffic interception functionality, as implemented by PWA, to quarantine an offending user and direct the user to the Quarantine Web Page for remediation.
  - The Quarantine Web Page may be served by any web server.
- The ToS-based PBR approach uses NetSight ASM and ToS rewrite to quarantine an offending user and seamlessly redirect its HTTP traffic using ToS-based PBR to the Quarantine Web Page for remediation.
  - The Quarantine Web Page is served by a specially configured device referred to as the "Proxy Engine".
- The SIP-based PBR uses NetSight ASM with custom scripting to quarantine an offending user and seamlessly redirect its HTTP traffic using SIP-based PBR to the Quarantine Web Page for remediation information.
  - The Quarantine Web Page is served by a specially configured device referred to as the "Proxy Engine".

In this example, the window shown in Figure 3 indicates that the PWA and the ToS-based PBR approaches are supported on the network, as designated by the corresponding check marks, based on the answers provided in the *AR Approach Selection* section. In this window, the Assisted Remediation approach(es) are selected for the second section of the ART, *AR Approach Configuration*. Note that although certain Assisted Remediation methods may not be supported on the network, they can be checked for the *AR Approach Configuration* section. This allows greater flexibility for the users of the tool.

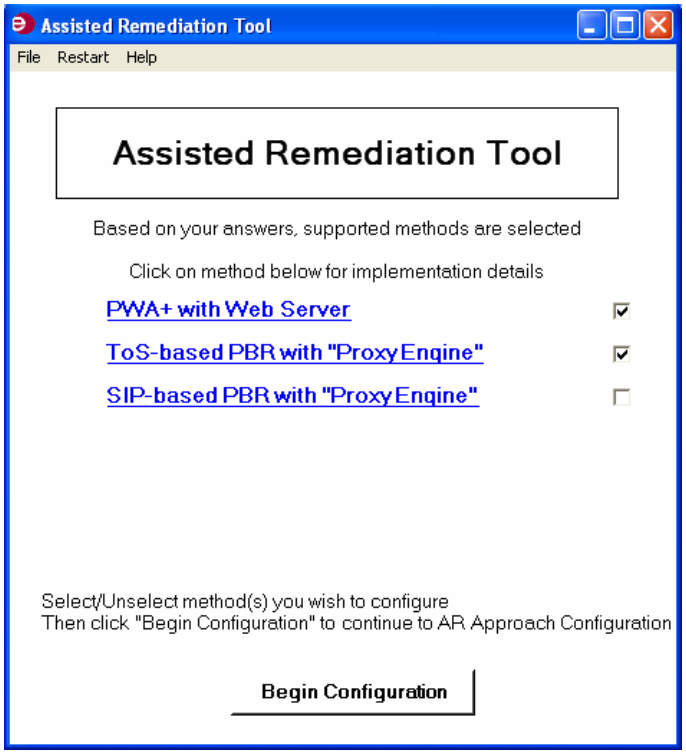

Figure 3. AR approach selection

Furthermore, to aid in the selection of an Assisted Remediation approach for enterprise deployment, clicking on an approach in the window shown in Figure 3 will pop up a new window describing some implementations details of the selected approach. Figure 4 shows the information displayed when the PWA approach is selected in the window shown in Figure 3.

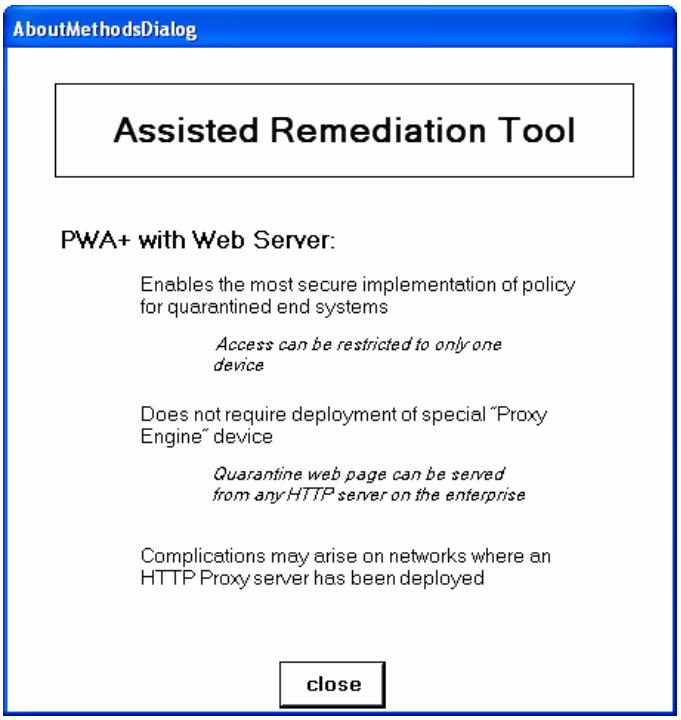

Figure 4. AR approach implementation details

After selecting the Assisted Remediation approach(es) for configuration on the network and clicking on *Begin Configuration* as shown in Figure 3, the deployment of Assisted Remediation is commenced. In this section, the user is prompted to input network configuration parameters needed for the Assisted Remediation implementation, and a step-by-step configuration guide is produced as the output. This configuration guide produces instructions for configuring network devices as well as automatically generated files used in the Assisted Remediation deployment.

Note that ART describes the configuration of Assisted Remediation under the assumption that the DIR Secure Networks Solution is already configured and has been fully deployed on the network. Therefore, ART assumes that Dragon is already configured for detecting the network security event for which Assisted Remediation is being implemented. Furthermore, the assumption is made that the Dragon Alarm Tool has been configured to send SNMPv3 Informs to NetSight ASM, using specific security parameters and ASM Event Category, for the network security event. ART will then specify the configuration of NetSight ASM based on these Dragon's settings for the deployment of Assisted Remediation.

The input parameter window in the *AR Approach Configuration* section of ART is where all the variables needed for Assisted Remediation implementation customization are entered. For example, Figure 5 shows the input parameter window for the PWA approach, which includes variables such as the PWA guest networking login credentials denoted by *Remediation Username* and *Remediation Password* as well as other variables. All fields in this window may be "moused" over for a brief description of the input variable.

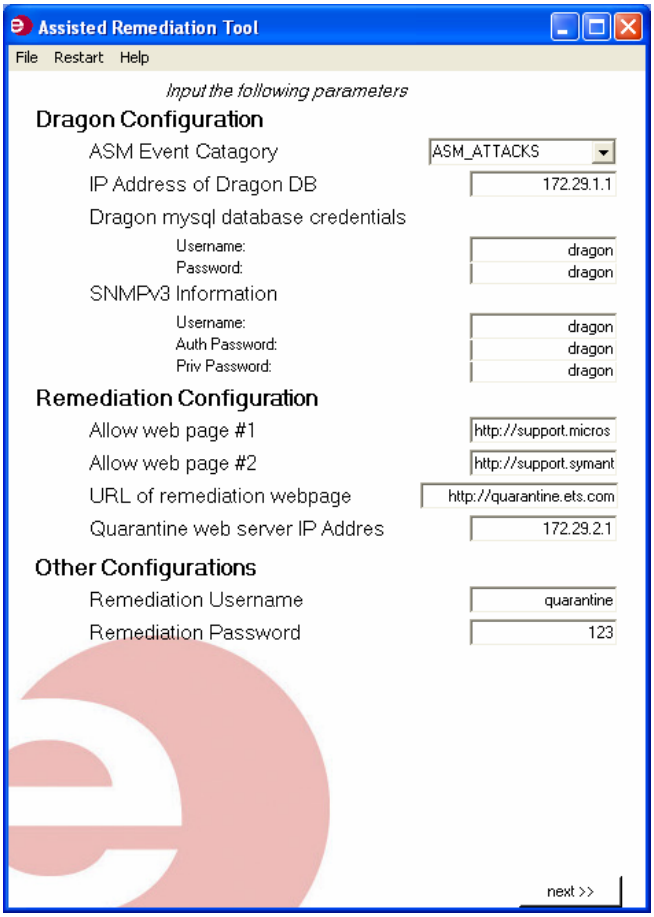

Figure 5. Input parameters for Assisted Remediation configuration

After the input parameters are entered, the *Next* button is used to start the configuration of the network infrastructure for Assisted Remediation. Each configuration step in ART is broken down into a "Task" which consists of configuring a single device or application on the network. For the PWA approach, the first task is configuring NetSight Policy Manager as shown in Figure 6. Each task simply lists configuration directions using the input parameters previously specified.

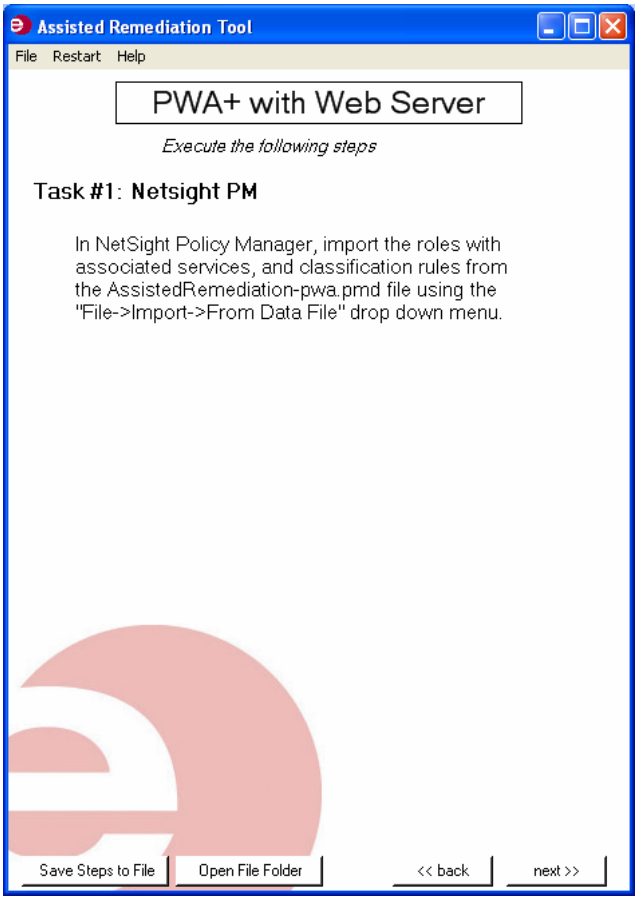

Figure 6. Task #1 for PWA approach configuration

Moreover, the task may reference a file to use for the network configuration. For example, the task shown in Figure 6 states to use the *AssistedRemediation-pwa.pmd* field in the configuration of NetSight Policy Manager. All files referenced in this section of the tool can be accessed by clicking on the *Open File Folder* button displayed at the bottom of the window. This button opens the local folder that contains all files automatically generated for Assisted Remediation deployment. Some of these files need to be manually modified by the user of the tool and these steps are explained by ART in detail. Other files need not be altered or may be automatically modified by ART based on the specified input parameters. The example displayed in Figure 7 shows that the file *squid.conf* does not need to be altered by the user of the tool, and the files *urls* and *index.php* have been automatically modified based on the indicated input variables.

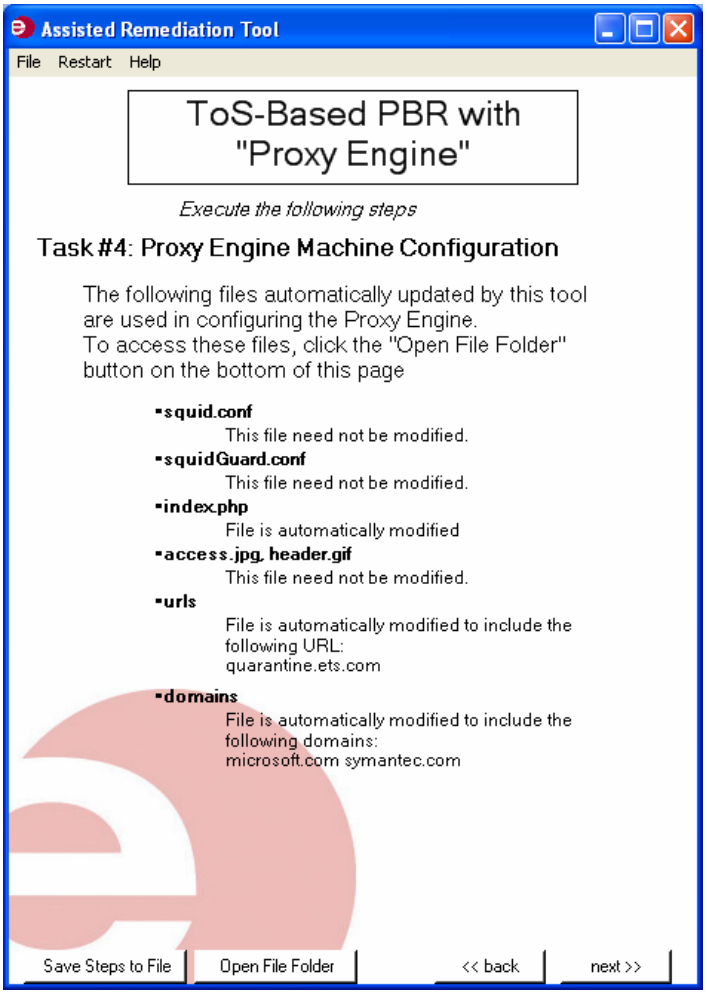

Figure 7. Task #4 for ToS-based PBR approach configuration

After the instructions are executed in each window, click on the *Next* button for the continuation of the task or the execution of a new task in the deployment of Assisted Remediation. Follow this sequence of windows until the end is reached where Assisted Remediation configuration is complete. Furthermore, it may be desired to generate a document that captures the entire sequence of steps explained in these windows. This file can be generated by using the *Save Steps to File* button, as shown in Figure 6 and Figure 7.

ART Configuration Details

For the PWA approach, the following tasks are executed for Assisted Remediation deployment:

- Task #1: NetSight Policy Manager
  - The *Quarantine_AR* policy role with the corresponding *Quarantine_AR* service and *Remediation* policy role with the corresponding *Remediation Services - Strict* service are automatically generated in the *AssistedRemediation-pwa.pmd* file.
  - These policy roles with corresponding services and classification rules are imported into the enterprise's current NetSight Policy Manager configuration and enforced throughout the network on infrastructure devices.
  - Classifications rules in the *Quarantine_AR* service and *Remediation Services – Strict* services are altered for enterprise customization.
  - Global settings of PWA enhanced mode are configured on access devices including guest networking and banner information.

- Task #2: NetSight ASM
  - Active Perl is downloaded and installed on the machine running NetSight ASM for the execution of the Perl scripts automatically generated by ART.
  - ATG tools are installed on this machine, which contains tools used by the ASM custom scripts.
  - Files *AR_Cfg_PWA.pl* and *AR_Undo_PWA.pl* are moved to ASM machine and an ASM rule is created using these custom scripts.
- Task #3: RADIUS Server
  - PWA guest networking credentials are added into the RADIUS server's database as a valid user, and associated to the Filter-ID of *Remediation*.
- Task #4: Dragon
  - Configurations to the mySQL database are made to allow a remote connection from NetSight ASM.
- Task #5: Quarantine Web Server
  - PHP is installed on web server serving Quarantine Web Page.
  - *Index.php*, automatically generated by ART, is the Quarantine Web Page and placed on any Web Server for displaying remediation information to quarantined end systems.

For the ToS-based PBR approach, the following tasks are executed for Assisted Remediation deployment:

- Task #1: NetSight Policy Manager
  - The *Quarantine* policy role with the corresponding *Remediation_TOS* service is automatically generated in the *AssistedRemediation-TOSPBR.pmd* file.
  - This policy role with corresponding service, classification rules, and Class of Service (CoS) are imported into the enterprise's current NetSight Policy Manager configuration and enforced throughout the network on infrastructure devices.
  - The ToS rewrite value is altered for the *Rewrite ToS_AR* CoS to the indicated value.
- Task #2: NetSight ASM
  - An ASM rule is created with the action being to apply the *Quarantine* policy role and the "Undo" action being to remove the *Quarantine* policy role.
- Task #3: Dragon
  - Configurations to the mySQL database are made to allow a remote connection from NetSight ASM.
- Task #4: Proxy Engine
  - The complete build of the Proxy Engine is stepped through from the installation of Linux Fedora Core 3 to the loading of Squid and SquidGuard on the machine and the configuration of NAT.
  - *Index.php* is automatically generated as the Quarantine Web Page to be placed on the Proxy Engine.
  - Additional files such as *urls* and *domains* are also automatically generated for loading on the Proxy Engine.
  - The Proxy Engine is connected to the network.
- Task #5: PBR
  - Policy based routing is configured on the router where the Proxy Engine is directly connected.

For the SIP-based PBR approach, the following tasks are executed for Assisted Remediation deployment:

- Task #1: NetSight Policy Manager
  - The *Quarantine* policy role with the corresponding *Remediation Services* service is automatically generated in the *AssistedRemediation-SIPPBR.pmd* file.

    - This policy role with corresponding service and classification rules are imported into the enterprise's current NetSight Policy Manager configuration and enforced throughout the network on infrastructure devices.
- Task #2: NetSight ASM
    - Active Perl is downloaded and installed on the machine running NetSight ASM for the execution of the automatically generated Perl scripts.
    - ATG tools are installed on this machine, which contains tools used by the ASM custom scripts.
    - Files *ASM_Add_ACL.pl* and *ASM_Remove_ACL.pl* are moved to the ASM machine and an ASM rule is created using these custom scripts.
    - Also, this ASM rule is configured with the action being applying the *Quarantine* policy role and the "Undo" action being removing the *Quarantine* policy role.
- Task #3: Dragon
    - Configurations to the mySQL database are made to allow a remote connection from NetSight ASM.
- Task #4: Proxy Engine
    - The complete build of the Proxy Engine is stepped through from the installation of Linux Fedora Core 3 to the loading of Squid and SquidGuard on the machine and configuration of NAT.
    - *Index.php* is automatically generated as the Quarantine Web Page to be placed on the Proxy Engine.
    - Additional files such as *urls* and *domains* are also automatically generated for loading on the Proxy Engine.
    - The Proxy Engine is connected to the network.
- Task #5: PBR
    - Policy based routing is configured on the router where the Proxy Engine is directly connected.

Conclusion

Assisted Remediation (AR) is designed to enable end-user notification that a quarantine action has been taken on their session. In order to aid in the configuration of Assisted Remediation on an existing enterprise network, the *Assisted Remediation Tool* (ART) was created as a deployment wizard for configuring Assisted Remediation with DIR. By using this tool, a network administrator is provided with a complete configuration guide to implementing Assisted Remediation on the existing infrastructure avoiding the configuration complexity of Assisted Remediation deployment. ART is available for download at the following link; ART download.

Please contact askthecto@enterasys.com for all inquiries concerning this article. Please contact enet-as@enterasys.com for all questions and comments concerning the operation of ART. To schedule Secure Networks Solutions Laboratory (SNSL) demonstrations of Assisted Remediation, please contact Sharon Berube. Click here to schedule a LiveView SNSL demonstration of Assisted Remediation.