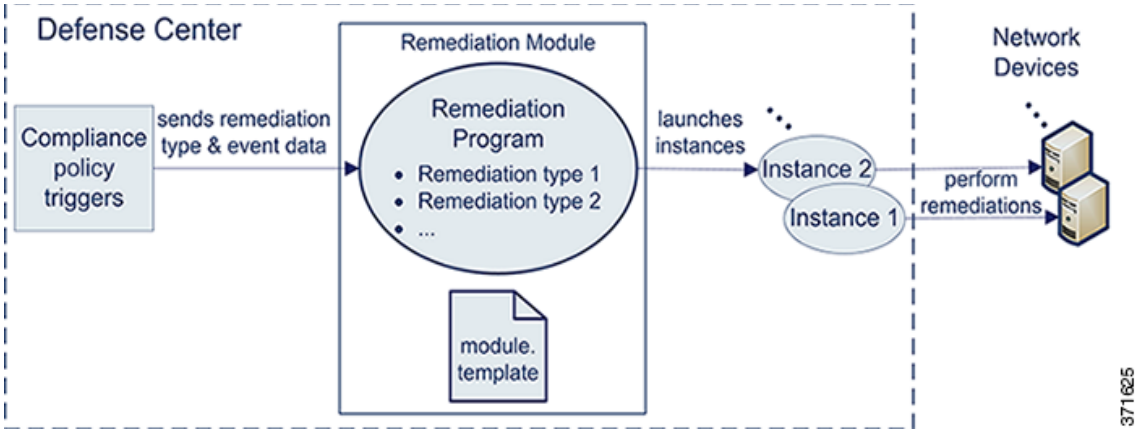
Understanding the Remediation Subsystem

The FireSIGHT System® remediation API allows you to create remediations that your Defense Center can automatically launch when conditions on your network violate the associated correlation policy. *A remediation is* the response your software program executes to mitigate the detected condition. For example, you can block traffic at a router on the source or destination IP address, or initiate a host Nmap scan to assess the host status. If multiple rules in a policy trigger, the Defense Center can launch responses for each rule. A *remediation module* is the package of files you install on the Defense Center to perform the response. A remediation module can incorporate several *remediation types* as shown in the graphic below.



For example, one of the system-provided remediation modules, the Cisco PIX router module, performs two remediation types: it either blocks packets by source IP address or blocks them by destination IP address.

If a remediation module targets multiple devices on your network (routers, hosts, and so forth), you configure your remediation module to perform multiple *instances*, one per device, when the correlation policy triggers. An instance is an instantiation of the remediation module, with one or more remediation types that correspond to functions in the remediation module code, and with a set of variables needed to run on the target device. For each instance, you specify the remediation type or types it executes and the instance-specific information such as the device's IP address and password for the remediation to access the target device on your network.

Prerequisites

Before using the remediation API for custom remediations, you should be familiar with information in the following categories:

FireSIGHT System

To understand the information in this guide, you should be familiar with the features and nomenclature of the FireSIGHT System, and the functions of certain components:

- the Defense Center role in the FireSIGHT System architecture
- correlation policy management module on the Defense Center
- remediation management module on the Defense Center

See the *FireSIGHT System User Guide* for further information.

Programming Requirements and Support

You must be able to code your custom remediation in Perl or shell script, or as a precompiled, statically-linked C program (with the exception of links to routines in glibc).

In addition, you must be able to produce a configuration file in XML for each remediation module. This file is called `module.template`. See the system-provided remediation modules for samples of this file. For module locations on the Defense Center, see Understanding the Remediation Subsystem File Structure, page 4-4.

For each instance you add, the Defense Center generates an instance-specific XML configuration file called `instance.conf`. Your code must parse this file each time a remediation instance executes.

The following table lists the packages available on the Defense Center as resources for writing and executing your remediation program.

Table 1-1 Additional Packages

Additional Packages	Location
GNU bash, version 3.2.33(1)-release	`/bin/bash`
tcsh 6.17.00	`/bin/tcsh`
glibc 2.7	`/lib/libc-2.7.so`
perl v5.10.1	`/usr/bin/perl`
Net::Telnet	`N/A`
Net::SSH::Perl	`N/A`
XML::Smart	`N/A`

Cisco-Provided Remediation Modules

The following table describes the predefined remediation modules included with the Defense Center. You should use these modules for reference when designing your remediation programs.

The system-provided modules are already installed on the Defense Center and include both the remediation executable (in Perl and C) and completed `module.template` configuration file for each module. For information on the easy steps to deploy system-provided remediation modules, see the *FireSIGHT System User Guide*.

Table 1-2 Cisco-Provided Remediation Modules

Module Name	Function
Cisco IOS Null Route	if you are running Cisco routers that use Cisco IOS® Version 12.0 or higher, allows you to dynamically block traffic sent to an IP address or network that violates a correlation policy
Cisco PIX Shun	if you are running Cisco PIX® Firewall Version 6.0 or higher, allows you to dynamically block traffic sent from an IP address that violates a correlation policy
Nmap Scanning	allows you to actively scan specific targets to determine operating systems and servers running on those hosts
Set Attribute Value	allows you to set a host attribute on a host where a correlation event occurs

The Remediation Subsystem

The remediation subsystem consists of the following components:

- the Defense Center's web interface, which you use to set up correlation policies and associate them with remediations, and to track the status of remediation processing
- the remediation API, which enables you to define the data that will be provided to your remediation modules
- the remediation daemon, which passed data to the remediation modules at run time and collects execution status information
- remediation modules, which perform specific responses to correlation policy violations

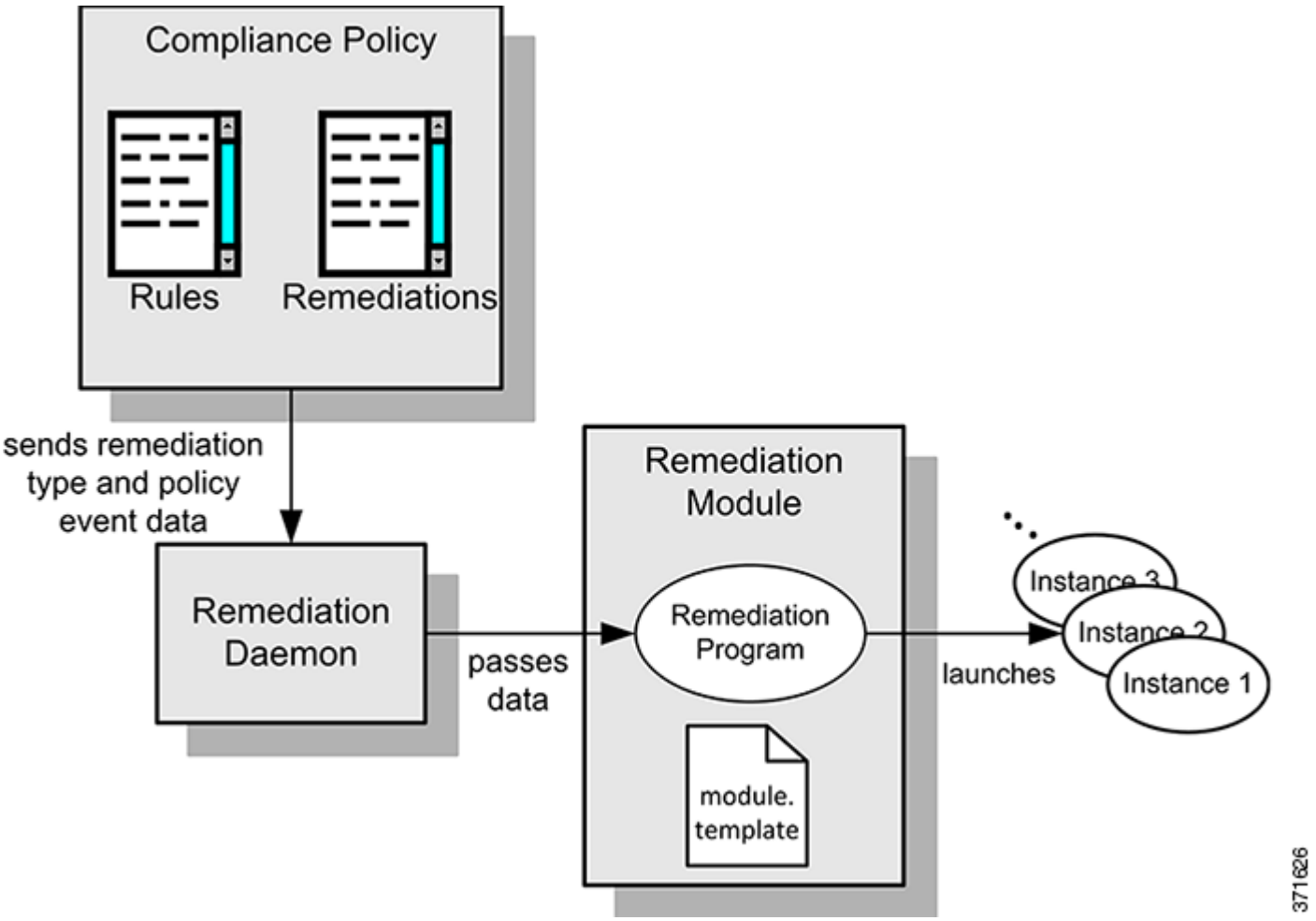
Understanding Remediation Subsystem Architecture

The remediation subsystem has a two-part architecture that is diagrammed in the figure below. The architecture consists of:

- infrastructure components such as the web interface and the remediation daemon which support all remediation modules. The infrastructure components allow you to create and manage all the remediation modules on your Defense Center. The remediation daemon manages the execution of the remediations. See Remediation Subsystem Components, page 1-3 for more details.
- the individual remediation modules which you develop to respond to specific correlation policy violations. See Remediation Module Architecture, page 1-4 for more details.

Remediation Subsystem Components

The following diagram illustrates the main functions of the remediation subsystem and their interactions.



You create remediations in order to respond to rule violations on your network in an automated mode. The Defense Center web interface allows you to define and activate your correlation policies and associate them with remediations. When a policy violation occurs, the remediation subsystem passes the name of the remediation and the event data specified in the `module.template` configuration file to the remediation daemon.

The remediation daemon launches the remediation and passes the correlation event data and instance-specific parameters to your remediation program. It also accepts return codes from the remediation program. The Defense Center uses the return codes for status displays.

The remediation program launches a set of *instances* of the remediation when the associated policy rule triggers. Each instance targets a particular network device. You create instances on the Instance Detail page of the Defense Center web interface. For each instance you provide the necessary instance-specific configuration details such as IP address and password of the target device.

Remediation Module Architecture

Each remediation module that you install on your Defense Center includes one or more remediation types. You assign one or more remediation types to each instance. For information on configuring remediations as responses to policy violations, see the Configuring Responses for Correlation Policies chapter in the *FireSIGHT System User Guide*.

Remediation modules include the following components:

- the remediation program, included in the remediation module package at installation. See Planning and Packaging Your Remediation Module, page 2-1.
- a required XML `module.template` file, also included in the remediation module package at installation. This file provides module-level information about your module and its data requirements that the remediation subsystem references each time it launches one of the remediation module's instances. See Communicating with the Remediation Subsystem, page 3-1.
- one XML `instance.conf` file per instance. The Defense Center auto-generates this file each time you configure a new instance of your remediation module.

Using the Remediation Subsystem

You deploy remediations by adding them as responses to specific rules in correlation policies on your Defense Center. You define the associations of correlation policies and remediations using the Defense Center web interface.

To deploy a remediation module, you must:

1. Identify the condition you want to mitigate and the actions that appropriately resolve that condition in your environment. These actions are the main functions your custom remediation program must implement.

   If you can use a Cisco-provided remediation module, skip directly to step 6.Install the module on the Defense Center using the web interface as described in Installing Your Module, page 2-13., page 1-5.
2. If you need to produce a custom remediation module, familiarize yourself with the data elements obtainable from the remediation subsystem. See Data Available from the Remediation Subsystem, page 2-1.
3. If you develop a custom remediation module you must also create a module template file to be included in your module package. See Communicating with the Remediation Subsystem, page 3-1 for the format and syntax of the file.
4. Write your remediation program so that it addresses all the functions necessary for the desired remediations. You can write your remediation module programs in bash, tsch, Perl or C. Develop your program using the technical guidance in Notes for Remediation Program Developers, page 4-3.
5. Package your remediation module as described in Packaging Your Module, page 2-12.
6. Install the module on the Defense Center using the web interface as described in Installing Your Module, page 2-13.
7. Ensure that the individual remediation types in your remediation module are assigned as responses to the correct correlation rules in your active correlation policies. See the *FireSIGHT System User Guide* for procedure details.

Remediation Resources

In addition to this document, other resources you can use to create your remediation modules include:

- a remediation SDK with sample program code in C or Perl that generates syslog alerts and demonstrates how a module can interact with your network. See Working with the Remediation SDK, page 4-1 chapter of this document for detailed information. The SDK can be downloaded from the Support site.

- the `module.template` schema (`module.template.xsd`), which is located on the Defense Center at `/etc/sf/remediation/module.template.xsd`.

The following table describes some of the topics explained in the documentation and where to look for more information.

Table 1-3 Remediation Resources

To learn more about...	See ...
the sample remediation module and the general procedure for creating, installing, and configuring one	Working with the Remediation SDK, page 4-1
writing your remediation program	Planning and Packaging Your Remediation Module, page 2-1
creating the `module.template` file	Communicating with the Remediation Subsystem, page 3-1
packaging your remediation module so you can install it on the Defense Center	Packaging Your Module, page 2-12
installing your remediation module	Installing Your Module, page 2-13
configuring your remediations as responses to security policy violations	the Configuring Responses for Correlation Policies chapter in the *FireSIGHT System User Guide*