Tivoli® SecureWay® Risk Manager

Integration Overview

Tivoli

What Is Tivoli SecureWay Risk Manager?

Tivoli SecureWay Risk Manager is an e-business security solution that enables customers to quickly manage threats, such as denial-of-service attacks and other forms of intrusions, across the enterprise. Distributed denial-of-service attacks on Amazon.com, CNN, and Yahoo in February 2000 increased awareness—and business—for intrusion-detection technology.

Not long ago, intrusion detection meant paying so-called "white hat" hackers to simulate break-ins on a company's network and search for clues of any real attempts. Now companies are under pressure to place full-time software sentries, or monitoring tools, at the hot spots in the network to continuously sniff out and deter intruders. Security experts[1] say the next round of hacker attacks will be more sinister, potentially taking down significant chunks of the Internet by exploiting DNS servers, HTML, and JavaScript code.

Although intrusion-detection and antivirus solutions perform different functions, an intrusion-detection tool might use techniques similar to those of an antivirus package to discover viruses in files. Each sensor looks for known "signatures" (such as sequences of network packets) or anomalies that might be caused by hacker tools and notifies the main intrusion-detection server if it finds any.

Problems arise because in a large network there is no such thing as normal traffic, and intrusion-detection sensors generate thousands of events, with many of them being false-positive or redundant information. Using leading intrusion-detection tools can make the number of alarms overwhelming. Many customers have indicated that intrusion-detection tools generate hundreds or thousands of events a day, and when an alarm sounds, no one knows what to do with it.

A new management platform is needed to centrally process information from multiple sensors and eliminate redundancy and false positives. Even if an attack has generated many intrusion-detection events across multiple sensors, Tivoli SecureWay Risk Manager includes an intelligent correlation engine that presents a single alarm per attack.

With Tivoli SecureWay Risk Manager you can also centrally monitor and manage all your security checkpoints from firewalls to antivirus products, from Web servers to database managers. You can intercept and resolve attacks and also centrally analyze all the relevant security alerts. Tivoli SecureWay Risk Manager supports continuous security improvement by identifying security "hot spots" in an enterprise network and by enabling effective correction of security policies that are affecting service levels and end-users' productivity.

The Value of Integration with a Total-Management Solution

Today's network-computing enterprise environment requires an open, centralized, scalable, and process-oriented approach to intrusion detection. Products such as firewalls, intrusion-detection appliances, access control, and Web servers are all required to implement specialized security functions. These products often do not interoperate with each other, must be managed and administered individually, and generate copious events and false alarms even

[1]Refer to the Computer Security Institute at www.gocsi.com

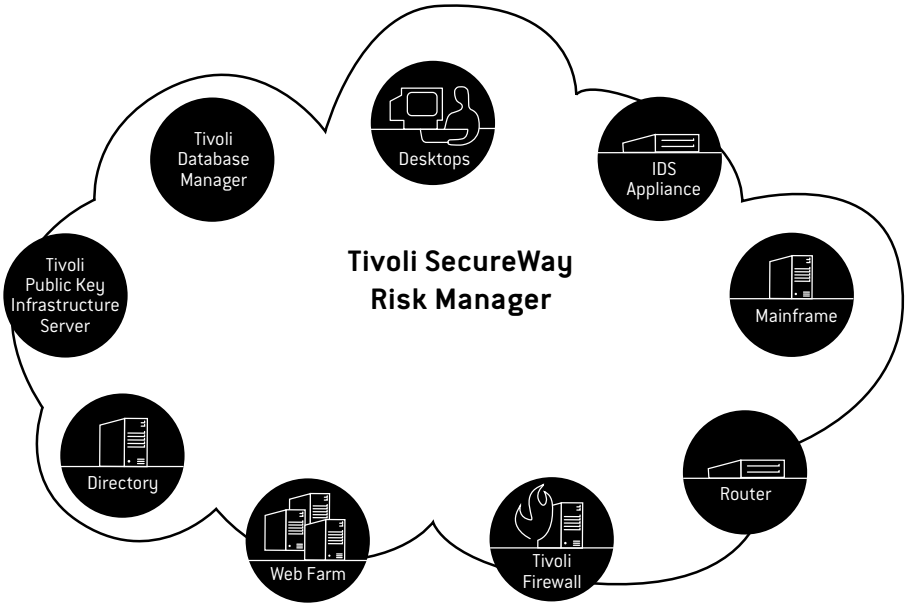

Figure 1. Tivoli SecureWay Risk Manager integrates information from multiple sources.

during normal operation. Because the security-device vendors lack an effective way of managing this data, administrators have to sift through the log file output from each intrusion agent and attempt a manual correlation—a laborious, time-consuming, and often error-prone process. Without centralized management, it is extremely difficult to determine attack patterns, make security assessments with any degree of assurance, or respond with real-time countermeasures. An integrated security solution is most effective when the firewalls, intrusion-detection agents, network security, and application-security solutions can work together in a coordinated fashion to minimize threats. Figure 1 illustrates Tivoli SecureWay Risk Manager integrating information from multiple sources.

According to Chris Jordan,[2] "When implementing intrusion-detection systems (IDS), large organizations must deal with a substantial collection of information that may be overwhelming. For example, OC-12 connections can generate about 850 megabytes of event data in an hour. How to collect and organize the incoming data is a significant issue in developing a large-scale IDS infrastructure."

Tivoli SecureWay Risk Manager is the first enterprise risk-management solution that enables you to:

- Implement a multi-tiered/distributed architecture with different layers of servers collecting data and sending only the relevant information to the upper level
- Pervasively manage and control all your enterprise-security checkpoints, including security products from firewalls to content-scanning tools and applications from database managers to Internet proxies
- Support centralized collection, correlation, and analysis of data but also react to attacks and resolve policy violations
- Implement role-based secure delegation of authority and define multiple administrators—roles responsible for first- or second-level analysis or for a subset of the network
- Make enterprise risk management a seamless part of your enterprise-management process to leverage the integration with a broad range of Tivoli and Tivoli Ready™ network- and systems-management products

[2]Refer to "Analyzing IDS Data" at www.securityfocus.com

- Protect and promote customers' investment in best-of-breed products and solutions. Tivoli SecureWay Risk Manager provides management capabilities that can be used with the base technology, such as firewall, IDS, or directory solutions, from other vendors.

Customer Environments

- Enterprise customers: Tivoli SecureWay Risk Manager is a cross-industry solution that helps enterprise customers manage threats, attacks, and other forms of intrusions across their enterprise.
- Service providers: Service providers can concurrently keep vigil over multiple networks and can obtain significant economies of scale by utilizing Tivoli SecureWay Risk Manager to provide intrusion-detection services.
- Mid-size companies: Tivoli SecureWay Risk Manager provides a simpler approach to security management by enabling existing employees to manage intrusions without requiring a large investment in more training.

Open Standards

Tivoli actively promotes, supports, and contributes to the emerging open-systems standards in the area of intrusion detection, including:

- The Common Intrusion Detection Framework (CIDF)[3]
- The Common Vulnerabilities and Exposures (CVE)[4]
- The Intrusion Detection Exchange Format (IDEF)[5]

CIDF enables different intrusion-detection and response components to interoperate and share information as richly as possible. These components include sensors that generate intrusion-related information; analysis engines that determine whether some anomaly or intrusion has occurred warranting a response; and response components, including network management, firewalls, filtering routers, and hosts. The CVE list is a dictionary of standardized names for vulnerability and other information. CVE standardizes the names for all publicly known vulnerabilities and security exposures. IDEF is a common intrusion-language specification that describes data formats and enables communication between intrusion-detection systems and management systems.

Tivoli SecureWay Risk Manager features a modular architecture compliant with the CIDF component model. The architecture comprises event generators, event analyzers, event databases, and response units. Tivoli SecureWay Risk Manager uses an IDEF-compliant data format for communication with intrusion-detection sensors. The current Internet draft of the IDEF data model was written by Herve Debar while he was working for IBM Research in the Global Security Analysis Lab in Zurich. This team developed the original prototype that led to the development of Tivoli SecureWay Risk Manager. The IDEF CLASSIFICATION Class names the vulnerability associated with the IDEF alert, and it includes the CVE identifier as one of its attributes.

[3]Refer to www.isi.edu/gost/cidf for more information
[4]Refer to www.cve.mitre.org for more information
[5]Refer to www.ietf.org/html.charters/idwg-charter.html for more information

Tivoli Ready Integration Requirements

A Tivoli Ready level of integration provides integration between an independent software vendor (ISV) application and Tivoli applications, such as Tivoli SecureWay Risk Manager. Tivoli open interfaces enable ISV applications to plug into the Tivoli product suite. An ISV application that has met the requirements for being Tivoli Ready is called a Tivoli Ready Module. For example, when an ISV application named XYZ has met the requirements for being Tivoli Ready, it can now be called *XYZ Tivoli Ready Module*. Tivoli Ready Modules provide integration between the ISV application and the Tivoli underlying framework and applications. Tivoli does provide some resources to assist with developing and marketing this integration, but Tivoli Ready Modules are developed, supported, and sold by an ISV or Team Tivoli Business Partner.

To integrate with Tivoli SecureWay Risk Manager at the Tivoli Ready level, an application needs to:

1. Send IDEF-compliant events to the Tivoli server via an event generator
2. Provide response units to allow the administrator to react to attacks or resolve exposures
3. Provide a Tivoli-compliant mechanism to install and configure event generators and response units

Tivoli SecureWay Risk Manager is built on top of the Tivoli Enterprise Console® (TEC), and it leverages the TEC application programming interface (API) for integration. Event generators should be implemented as Tivoli event adapters, and response units should be implemented as Tivoli tasks.

TEC provides an extensible means for collecting and integrating disparate management information into a common model for event processing and a central-operations view. Types of event processing include event correlation, filtering, dropping duplicates, prioritizing, consolidating, closing self-correcting events, escalating events, and forwarding events. TEC handles events from applications, databases, and systems and network devices. After events are defined, TEC rules can correlate events and define automated actions. Correlation automatically closes events related to problems that have been resolved. Automation resolves problems with no user intervention.

IDEF-Compliant Event Adapters

An adapter is a process that monitors resources so that the resources can be managed. When an adapter detects an event generated from a monitored resource, it puts the event in IDEF and sends it to the server. The event server then further processes the event.

Adapters can monitor resources in the following ways:

- An adapter can receive events from any source that actively produces them. For example, SNMP adapters can receive traps sent by the Simple Network Management Protocol (SNMP).
- An adapter can check an ASCII log file, the UNIX® Syslog file, or the Windows® system log files for raw events if the monitored resource updates a log file with messages.

Tasks

A task is a function that can be executed once or on a routine basis. Tasks enable an administrator to securely define a set of complex operations that can be run easily on different machine types. Tivoli SecureWay Risk Manager can execute tasks on Tivoli-managed workstations and display the results of these tasks on the Tivoli desktop. Results also can be stored or redirected to a file. Tasks can be written in any low-level language (for example, C/C++), but often they are platform-neutral PERL scripts, DOS or Windows batch files, or UNIX shell scripts that invoke some components already available in the product being integrated.

Installation and Configuration

TEC uses the Adapter Configuration Facility (ACF) to configure, customize, and distribute event adapters. The list of files and the configuration information required to install and configure an adapter are provided to ACF via adapter configuration profiles (ACP). You can store your ACP definition in an ASCII file and import it into ACF via a command line interface (CLI).

Tasks also can be imported into Tivoli SecureWay Risk Manager via a CLI by just providing the task name and its parameters.

System Requirements

Tivoli Ready Modules manage an integrated application from any Tivoli platform. Typical tier-1 platforms supported by Tivoli Ready products are AIX®, Windows NT® and Windows 2000, Sun Solaris™, and HP-UX.

ISV applications do not have to run on all Tivoli-supported platforms, but the Tivoli Ready Module integration must allow management tasks to be performed on each Tivoli-supported platform. For example, ISV application XYZ may run only on Windows NT, but the integration included in the XYZ Tivoli Ready Module allows an administrator to analyze events and execute a task from any Tivoli desktop. For this reason, Tivoli Ready Modules are tested on all Tivoli-supported platforms during certification.

Estimated Completion Time in Business Days

Activity	Estimated Number of Days
Formal Training	2
Hardware and Tivoli Set-Up	5
Development	5 – 15
Internal Testing and Quality Assurance	5
Tivoli Certification	1

Manage. Anything. Anywhere.™

Printed in the U.S.A. XXXXXXX XX-XXXXXX-XX www.tivoli.com