

Foundstone Enterprise's Distributed Scanning Capabilities

Overview

Large organizations possess complex networks that often span wide geographic boundaries. Unfortunately, the links that connect these enterprises sometimes offer varying degrees of bandwidth and reliability. Network filtering is also common, making it impossible to gain a complete view of the organization from a single vantage point.

Foundstone Enterprise™ accommodates these scenarios by employing multiple FoundScan Engines distributed throughout an organization. Controlled via the Foundstone Enterprise Manager, FoundScan Engines report their results to the Foundstone Database. This architecture provides customers with centralized administration and reporting and the ability to implement a scanning regimen that best fits their environment.

Challenges of Distributed Networks

The architecture of modern distributed networks can make it difficult to perform complete, enterprisewide scanning. Network connections are occasionally unreliable or have limited bandwidth. Firewalls, routers, and other network devices add a layer of filtering, while network usage policies and localized device management present other complications.

Scanning must also meet the requirements of modern security management. Vulnerability findings (regarding the payroll server or a sales database, for instance) are extremely sensitive, and this data must be centrally located and secured. The stakes are too high to have this information in an unencrypted email inbox, strewn across multiple laptops, or even printed out on someone's desk.

Vulnerability data must also be controlled from one location to enable integration with other security products (IDS and Security Information Management, for example) and to perform sophisticated pattern and trend analysis.

A Distributed Architecture for Distributed Networks

Foundstone Enterprise utilizes three major components to meet the needs of large distributed organizations:

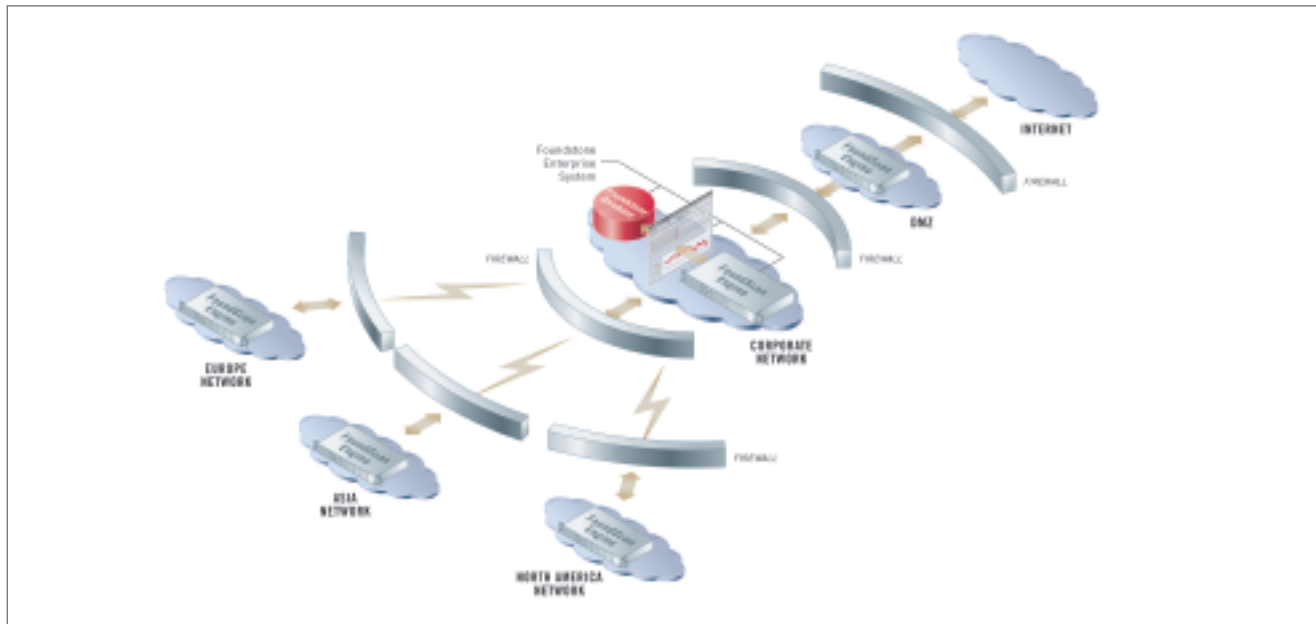
- **Foundstone Enterprise Manager:** This web portal provides a centralized view of the entire vulnerability management process—from asset discovery and prioritization, to monitoring, remediation, and reporting.
- **FoundScan Engine™:** Foundstone's core scanning technology enables asset discovery and vulnerability analysis across the enterprise
- **FoundScan Database:** This scalable, constantly updated repository integrates organization-specific data (assets, vulnerabilities, and threats) with Foundstone's knowledge base built from years of real-world experience.

In a typical environment, FoundScan Engines are deployed in strategic locations throughout the network and centrally controlled via Foundstone Enterprise Manager. The administrator gets both flexibility (access from anywhere) and security (authenticated, encrypted sessions).

Using Foundstone Enterprise Manager, the administrator simply selects a particular FoundScan Engine to run a scan. During a scan, the FoundScan Engine sends data to the Foundstone Database in regular batches, instead of swamping the network with results upon scan completion. This is especially important when running large scans. Administrators can track scans running on all FoundScan Engines with the Foundstone Enterprise Manager, as well as check the status of each FoundScan Engine.

All system communication in Foundstone Enterprise can use a single, common port (i.e., SSL), which permits secure transmissions without the need to of modify firewall rules. Foundstone Enterprise uses an open, web services model for communication, enabling flexible interaction between its components and smooth integration with other technologies.

Foundstone Enterprise Distributed Scanning Architecture



Centralized Vulnerability Updates

Thanks to centralized updating and an intelligent distributed architecture, Foundstone Enterprise is always up-to-date with the latest security threats and exploits. The automated update feature downloads the most recent vulnerability checks and data from Foundstone at regular, configurable intervals. The data is immediately added to the Foundstone Database and available to all FoundScan Engines.

Prior to performing a scan, the FoundScan Engine automatically requests the latest vulnerability checks from the Foundstone Database. There's no danger of missing the most recent security threats. Automatic updating also eliminates the headache of manually keeping a vulnerability management system current, which wastes bandwidth, manpower, time, and other valuable resources.

Network-Aware Availability Detection

Foundstone Enterprise includes network connectivity features that meet the challenges of scanning across highly distributed networks, where even the most reliable links can become temporarily unavailable. Traditional products are unaware of link failures and continue scanning. They eventually time out on the remaining hosts, providing incomplete reports with inaccurate results.

The Network Connectivity Detection capability in Foundstone Enterprise allows an administrator to specify a target remote host (such as a core router) to continually monitor. If this host becomes unreachable, Foundstone Enterprise automatically pauses scans that are running, and then resumes them when connectivity is restored. Foundstone Enterprise also detects when connection between the FoundScan Engines and the Foundstone Database is interrupted. Results are queued on the FoundScan Engines until connectivity is restored. By detecting the availability of network and system connections, Foundstone Enterprise ensures scan accuracy and completion.

Copyright 2003 Foundstone, Inc. All Rights Reserved.

Foundstone Enterprise Manager, Enterprise Risk Solutions (ERS), Foundstone Scripting Language (FSL), FS1000, Foundstone Enterprise, FoundScan Engine, FS1000 Appliance, Foundstone Managed Service, Foundstone Professional, Foundstone Professional TL, and the Foundstone name are trademarks of Foundstone, Inc. All other company, brand and product trademarks, registered trademarks and service marks are the property of their respective owners.

CALL 1.877.91.FOUND

WWW.FOUNDSTONE.COM