SecurityCenter 4.4
Architecture
September 21, 2012
(Revision 2)

The newest version of this document is available at the following URL:
http://static.tenable.com/prod_docs/SecurityCenter_4.4_Architecture.pdf
# Table of Contents

**Introduction** .................................................................................................................. 4
  Standards and Conventions ......................................................................................... 4
  Abbreviations .............................................................................................................. 5

**SecurityCenter Functions** .......................................................................................... 5
  Vulnerability Discovery and Management ................................................................... 7
    *Vulnerability Repositories* ..................................................................................... 7
    *Data Acquisition Methods* .................................................................................... 8
  Security Event Management and Incident Response .................................................. 8
    *Anomaly Detection* ............................................................................................... 9
    *Intrusion Detection and Vulnerability Correlation* .............................................. 9
    *Rules-based Event Correlation* ................................................................. 10
  Measuring and Demonstrating Configuration Management ....................................... 10
    *Configuration Auditing* ...................................................................................... 10
    *Rogue Host Detection* ......................................................................................... 11
    *Measurable Security Management Program* ...................................................... 11
  Continuous Network Monitoring and Discovery ......................................................... 11
    *Dynamic Asset Discovery* .................................................................................... 11
    *Static Asset Management* .................................................................................... 11
    *Watchlists* ........................................................................................................... 11
    *Asset-Based Workflow, Access Control, and Reporting* .................................... 12

**SecurityCenter Components** ...................................................................................... 12
  Nessus Scanners ......................................................................................................... 12
  Passive Vulnerability Scanner .................................................................................... 13
  Log Correlation Engine .............................................................................................. 13
  Third-Party Data Sources (IDS Events and Log Sources) ........................................... 14
  Supported Operating Systems and Environments ....................................................... 14
  SecurityCenter Communications and Repositories ...................................................... 16

**Architecture** .................................................................................................................. 19
  Virtualized Environments ............................................................................................ 19
  Single Server Architecture ........................................................................................... 19
  Multiple Scanner Architecture ..................................................................................... 21
  Single Log Correlation Engine Architecture ............................................................ 23
  Multiple Log Correlation Engine Architecture ......................................................... 24
  Multiple SecurityCenter Architecture ......................................................................... 24

**User Management** ....................................................................................................... 25
  Organizational Security Model .................................................................................... 26
    *Defining Single or Multiple Organizations* ......................................................... 28
  Users and Roles ........................................................................................................... 28
    *User Visibility* ....................................................................................................... 29
    *Access Control* ..................................................................................................... 30

**Asset Management** ..................................................................................................... 32
INTRODUCTION
Tenable’s SecurityCenter is a web-based management console that unifies the process of vulnerability detection and management, event and log management, compliance monitoring, reporting and flaw remediation. SecurityCenter enables efficient communication of security events to IT staff, management and audit teams.

This document describes the SecurityCenter architecture and provides a high-level view of how its components interact.

Since many of Tenable’s customers have requirements to maintain separation of duties, the SecurityCenter 4.4 documentation has been separated into the following documents to better organize the material based on the organizational role. Note that there may be some overlap in roles as well as content provided with each of the following guides:

- **SecurityCenter 4.4 Architecture** – This document describes the SecurityCenter architecture and provides a high-level view of how the components interact. This document is beneficial for those who are considering purchasing SecurityCenter.

- **SecurityCenter 4.4 Installation Guide** – This document provides instructions for the installation of SecurityCenter 4. The target audience for this document is system administrators who need to install the SecurityCenter application. Included in this document are quick instructions for the admin user to add a Nessus scanner and create a user account to launch a test scan to ensure SecurityCenter is correctly installed.

- **SecurityCenter 4.4 Upgrade Guide** – This document describes the process of upgrading to the latest version of SecurityCenter.

- **SecurityCenter 4.4 Administration Guide** – This document provides instructions for the administration of SecurityCenter by the admin user. The admin user is the first user to log into the SecurityCenter after the initial installation and is responsible for configuration tasks such as defining organizations, repositories, Nessus scanners, LCE servers and PVS sensors. The admin user does not have the ability to create and launch Nessus scans.

- **SecurityCenter 4.4 User Guide** – This document provides instructions for using SecurityCenter by an Organization Head user or lesser account.

Please email any comments and suggestions to support@tenable.com.

A basic understanding of Linux/Unix, Windows, vulnerability scanning with Nessus, intrusion detection, and log analysis is assumed.

STANDARDS AND CONVENTIONS
Throughout the documentation, filenames, daemons, and executables are indicated with a courier bold font such as gunzip, httpd, and /etc/passwd.

Command line options and keywords are also indicated with the courier bold font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in courier bold to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Unix pwd command:

```
# pwd
```
/opt/sc4/daemons
#

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples, and best practices are highlighted with this symbol and white on blue text.

**ABBREVIATIONS**
The following abbreviations are used throughout this documentation:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCE</td>
<td>Log Correlation Engine</td>
</tr>
<tr>
<td>PVS</td>
<td>Passive Vulnerability Scanner</td>
</tr>
<tr>
<td>SC</td>
<td>SecurityCenter</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
</tbody>
</table>

**SECURITYCENTER FUNCTIONS**
Tenable Network Security, Inc. was founded on the belief that it is crucial to monitor systems in a manner as close to real-time as possible to ensure organizations do not drift out of compliance over time. The greater the gap between monitoring cycles, the more likely it is for compliance violations to occur undetected. Tenable’s solutions can be customized for a particular organization’s requirements and then automatically provide a unified view of the security status through a single management interface that is continually updated with the latest information.

Tenable’s SecurityCenter (US Patent No. 7,926,113 B1, “System and Method for Managing Network Vulnerability Analysis Systems”) facilitates a measurable increase in network security by performing the following core functions:

- Vulnerability discovery and management
- Security event management and incident response
- Measuring and demonstrating configuration management
- Continuous network monitoring and discovery

Tenable offers a SecurityCenter bundle called Continuous View, which provides a method for reviewing results of networks which are scanned actively using Nessus and passively using the Passive Vulnerability Scanner (PVS). Utilizing both active and passive scanners allows for a more complete view of the network. Please note that LCE features are not included in Continuous View but may be purchased separately. If you have not purchased the LCE option, please ignore references to LCE in the SecurityCenter documents.

Tenable also sells a product called the “LCE Manager” that is very similar to the SecurityCenter web interface except that it supports event management capability only. This product also supports a single repository/organization only.
The information from each of these disparate disciplines is centralized with a common reporting, ticketing, user-interface and security model.

By unifying this data into one centralized source, SecurityCenter ensures that the right people in any organization have the information they need to make informed decisions.

SecurityCenter implements a hierarchical approach to object access that scales well to large organizations and facilitates complex inter-organizational access and security.

The following is an example SecurityCenter dashboard tab. The network has been segregated into several different assets such as the "Linux Assets" and "Windows Assets". Also displayed are activity trends and detected intrusion events along with other important data. Dashboard components are configured by organizational users harnessing the ability of the SecurityCenter to compute the total amount of security events and vulnerabilities for each asset and generate useful displays.

Example Dashboard View

Both simple and powerful, this report is available on a hierarchical level such that each user and group sees a unique report within their own login page. For example, senior managers can see the high level trends for the entire network while network administrators can see how a few of their routers compare to their mail servers. The data behind each component
is readily available by drilling down from the dashboard view to the underlying vulnerability or event data. This availability along with configurable alerting facilitates real-time discovery and rapid response to security issues. For more information on the dashboard along with sample tabs built by Tenable and other SecurityCenter users, please visit the SecurityCenter Dashboard site at: http://blog.tenable.com/sc4dashboards/.

VULNERABILITY DISCOVERY AND MANAGEMENT

It is important to monitor systems for vulnerabilities in as close to real-time as possible. Penetration tests can discover vulnerabilities in the IT infrastructure, but they are only a snapshot in time. A system that is scanned and found to be free of vulnerabilities on one day may be completely exploitable the next day. SecurityCenter provides a comprehensive approach to vulnerability discovery and management through vulnerability repositories and multiple data acquisition methods such as passive vulnerability discovery and scan scheduling.

Example list of top vulnerabilities

Vulnerability Repositories

Repositories are an excellent way to logically divide vulnerability data up based on organizational needs. For example, three repositories could be created: one for “active” vulnerabilities, one for “passive” vulnerabilities and a third for “compliance” data. Repositories can also be created based on geographical locations, asset importance, user types, etc.

A repository is essentially a database of vulnerability data defined by one or more ranges of IP addresses. SecurityCenter integrates repositories of vulnerability data that are shared as needed among users, organizations and other SecurityCenter consoles. Vulnerability data is maintained in a hierarchical fashion with descending layers of permission levels. What this means simply is that every user who has role permissions that allow them to create other
users can create a new user and assign a subset of their own repositories, assets and resources to the new user. The new user, assuming they have the appropriate role permissions, can then create other users with a subset of their allocation.

This hierarchical layering of repository storage makes vulnerability data extremely scalable in large organizations and highly configurable for complex organizational structures. Repositories can also be shared between multiple SecurityCenters. This sharing of repositories supports the concept of tiered consoles where one SecurityCenter may have a subset of the repository information from another SecurityCenter.

**Data Acquisition Methods**
SecurityCenter uses multiple methods to acquire data to provide a comprehensive view of the organization’s security posture. Data is acquired through active vulnerability scanning, agent-less patch auditing, log correlation integration, and continuous passive discovery.

**Active Vulnerability Scanning**
SecurityCenter can manage one or more Nessus vulnerability scanners. Scan policies that discover new hosts, new applications, and new vulnerabilities can be scheduled and automatically distributed to multiple scanners for load balancing. SecurityCenter manages which Nessus scanners are best suited to scan a particular host and can also use a remote Nessus scanner to simulate what an external person might see.

**Agent-less Patch Auditing**
Nessus credential scans can be leveraged to perform highly accurate and rapid patch, configuration, and vulnerability audits on a large variety of servers and devices. Credentialled scans can also enumerate all UDP and TCP ports in just a few seconds. SecurityCenter can securely manage these credentials across thousands of different systems and share the results of these audits only with users who have a need to know.

**Continuous Passive Discovery**
SecurityCenter can also manage one or more Tenable Passive Vulnerability Scanners (PVS). PVS provides continuous discovery of new hosts, new applications, and new vulnerabilities. It runs 24x7 and discovers highly accurate client and server vulnerability information. SecurityCenter fuses this information with the active or credentialled scan results from Nessus.

**Security Event Management and Incident Response**
A documented and tested incident response plan is necessary to ensure the prompt detection, identification, mitigation, and analysis of all security incidents. SecurityCenter aids in the incident response process in the following two strategic areas:

- Detecting the incident
- Responding quickly to an incident

The ability to detect an incident efficiently in an automated manner is often overlooked. Most automation for detecting incidents generates many false positives that make the process unreliable and time consuming. Tenable’s approach is to correlate many types of data along with known system configuration and vulnerabilities and generate relevant alerts that get sent to personnel who need them the most.

When an incident is reported externally (e.g., through a help desk phone call), having all network activity, system logs, configuration data, and firewall logs at an analyst’s fingertips
can help them quickly categorize the type of incident they are dealing with. When an analyst detects a potential compromise, abuse, or other type of anomaly with SecurityCenter, they typically have enough information to make a determination to start an incident response exercise.

The ability to respond to an incident correctly and quickly is critical to limiting and remediating any exposure from an incident.

**Example summary of all IDS events**

### Anomaly Detection

SecurityCenter has an optional, but important, component called the Log Correlation Engine (LCE) that allows it to take log events from a wide variety of devices such as firewalls, routers, honey-pots, and web servers. LCE includes an anomaly engine that looks for large changes in behavior that may be indicative of a system compromise or abuse.

### Intrusion Detection and Vulnerability Correlation

SecurityCenter can also analyze IDS events from the LCE, check to see if the target of an event is vulnerable to the attack and then distribute this information to the system administrators responsible for the asset. The LCE receives IDS events from a variety of sources and correlates the events based on vulnerability data received from SecurityCenter. When an IDS event is received that targets a vulnerable system, SecurityCenter can send an email message to the affected users as well.

Organizations that make use of SecurityCenter and the LCE can quickly provide a global picture of system activity to those responding to an incident. The PVS is also useful for discovering up-to-the-minute configuration data on potentially compromised hosts.

SecurityCenter provides the ability to save all LCE data from a suspected incident in a separate report that aids in the analysis phase of incident response.
All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence if required. Previous searches can also be re-launched against a new data set to update the log data.

**Rules-based Event Correlation**

LCE also includes an event scripting language based on Nessus’ NASL language. This language is called the Tenable Application Scripting Language (TASL) and can be used to perform complex correlation tasks in real-time. Example scripts include the ability to alert for all login and login failures that occur after hours and on the weekends or when a host is attacked and then makes a connection to a known blacklisted IP address. In addition, TASL provides discovery and alerts based on previously unseen Ethernet addresses in the logs from a Windows DHCP server.

**MEASURING AND DEMONSTRATING CONFIGURATION MANAGEMENT**

Configuration standards for desktops, laptops, and servers provide consistency throughout the organization. For example, the Center for Internet Security (CIS) has benchmarks that provide consensus guidelines for securing a number of applications and OS platforms. Tenable provides automated system compliance audits based on many of these benchmarks along with a variety of other security industry standards.

**Configuration Auditing**

With the use of a Nessus credentialed scan, multiple Unix, Windows, Mac OS X, database, and Cisco nodes can be audited against a specific set of configuration guidelines. Tenable provides a set of common audit guides implemented for use in various enterprise, financial, health care, and government audits. SecurityCenter can help detect and measure violations to an established desktop and server configuration management policy.

SecurityCenter can be used to assess specific asset classes of servers or desktops with specific configuration audits. Audits can be performed against:

- Red Hat, Solaris, AIX, HP-UX, Debian, SuSE and FreeBSD
- Oracle, MySQL, MS SQL, DB2 and PostgreSQL
- Applications such as IIS, Apache, Nessus and more

Tenable’s list of pre-configured configuration audit files include but are not limited to:

- USGCB and SCAP audits
- DISA STIG audits
- CIS audits for Unix, Windows, Mac OS X, Cisco and VMWare
- Microsoft vendor recommendations
- PCI DSS configuration settings
- Antivirus configuration
- Malware detection

Audits are performed entirely through credentialed checks and do not require the use of an agent.
Rogue Host Detection
Real-time network analysis as well as regular active scanning can discover new hosts that must be audited. SecurityCenter uses time indexing to determine when systems and vulnerabilities are first discovered and when they were last seen. Whether an organization is using one Nessus scanner, multiple scanners, or continuously receiving vulnerability reports from a PVS, any SecurityCenter user can see what has been discovered at any time with the click of a button.

Measurable Security Management Program
Auditors seek to understand the effectiveness of a security management program. With SecurityCenter, users can demonstrate to auditors when security issues were first identified, what was done to inform system owners of their required actions (such as disabling an unauthorized service), and how long it took to close an issue. SecurityCenter includes trending and reporting tools that can help demonstrate the types of security deficiencies that can be fed back into a security management program.

For example, an organization may have a policy requiring that patches be applied within 30 days of release. SecurityCenter can monitor compliance with this policy and provide metrics to determine how the business units compare. This helps determine which business units may need more training on the risks to the organization when patches are not applied.

Continuous Network Monitoring and Discovery
Real-time network monitoring enables organizations to proactively correct compliance violations before they become a problem. If violations are detected and corrected prior to an actual audit, the audit results will reflect positively on the organization. SecurityCenter provides several methods to identify and monitor assets in an automated manner.

Dynamic Asset Discovery
SecurityCenter has the ability to parse the results of any Nessus or PVS data obtained and build dynamic lists of IPs. For example, a dynamic rule can be created that builds a list of IP addresses that each had port 80 and port 25 open. These rules can be very sophisticated and take into account addressing, open ports, specific vulnerability IDs and discovered vulnerability content. SecurityCenter ships with many example dynamic rules. Additionally, new rules can be created easily within the application.

Static Asset Management
Dynamic asset lists can be augmented with existing static repository lists. For example, if a source of asset information exists outside of the SecurityCenter, it can be uploaded as often as needed. Another example might be where a network management system produces a report of all managed Cisco routers. This list can be added to the SecurityCenter and used immediately.

Watchlists
SecurityCenter 4 provides an asset list type known as a “Watchlist”. A Watchlist is an asset list, meant only for events, that is used to maintain lists of IPs not in your managed range of IP addresses. This proves beneficial when analyzing event activity originating outside of your managed range. For example, if a block of IP addresses is a known source of malicious activity, they could be added to a Watchlist called “malicious IPs” and added to a custom query. Normally IPs outside of your managed range would not appear within your list of viewable events.
Asset-Based Workflow, Access Control, and Reporting
All SecurityCenter functions are controlled by asset lists. Individual SecurityCenter users are assigned one or more asset lists, which can be either static or dynamic. Users who have the ability to scan can only scan hosts in their asset lists. Similarly, users can only see vulnerability or compliance data for systems within their asset groups.

SECURITYCENTER COMPONENTS
The Job Scheduler (Jobd) process manages the scheduling of all system tasks such as launching vulnerability scans, sending email, importing vulnerability information, generating reports, and new IDS signature and Nessus plugin downloads.

Tenable includes the Apache web server as part of the SecurityCenter RPM distribution. Apache is used to present the user and administration interface. By default, Tenable ships the SecurityCenter’s Apache web server with only the HTTPS protocol enabled.

SecurityCenter stores all of its vulnerability and intrusion data into highly optimized, proprietary-format binary files. Other data, such as organization and user data, is stored in an indexed SQLite format.

SecurityCenter and all supporting components are initialized post operating system start-up and are not initiated as a single homogeneous process, but rather as discrete init-based daemons that listen on predefined ports (see Appendix 1: Tenable Data Flow Diagram) for inter-process communication and interact securely with each other after their initialization is complete.

The system components are managed securely due to the fact that they operate under a non-login based user and require a user with root-level privileges to perform any critical operations such as stopping, starting or restarting the initialized processes. Communication security is maintained, as specified on pages 16-18 of the SecurityCenter Architecture Guide, by the encryption of all inter-process communications.

SecurityCenter sends all email through an external SMTP server. The administrator user configures the desired SMTP settings including hostname, port, authentication method, secure connection, and return address, and the Jobd scheduler kicks off the email process as necessary. Multiple forms of authenticated email are supported and many types of emails can be sent such as attack alerts, text results of new vulnerability scans, and scheduled PDF reports. SecurityCenter does not have a daemon listening for incoming email.

NESSUS SCANNERS
Nessus is a powerful, up-to-date and easy-to-use network security scanner. It is currently rated as the top product of its type throughout the security industry and is endorsed by professional information security organizations such as the SANS Institute. Nessus allows you to remotely audit a given network and determine if it has been compromised or misused in some way. Nessus also provides the ability to locally audit a specific machine for vulnerabilities, compliance specifications, content policy violations, and more.

Nessus consists of two major components: the server and the User Interface (UI). Standalone Nessus scanners use a web-based interface made up of a simple web server and web client to manage scans. SecurityCenter provides the UI for managed Nessus scanners.
When a Nessus UI connects to the Nessus daemon, it establishes an SSL-protected connection and authenticates with either a certificate or a username and password. The Nessus UI passes the daemon a list of vulnerability checks, a set of IP ranges to test, and parameters to conduct a test. The daemon conducts the test and sends the results back to the UI as they are available. To a Nessus scanner, a scan sent to it by SecurityCenter is no different than performing a scan sent to it by the Nessus web interface.

SecurityCenter is smart enough to perform load balancing between available scanners, only use certain scanners for portions of the topology and, if desired, use the “wrong” scanner on purpose to simulate attacks from the outside world.

Although Tenable continues to make the Nessus scanner as fast and efficient as possible, using multiple scanners can dramatically reduce the amount of time to complete a scan. Multiple scanners can also cause less stress to VPN links, routers, and other network devices by placing scanners closer to their targets.

SecurityCenter deployments are IP-based and not licensed per scanner. This allows you to deploy as many scanners as needed to ensure enterprise-wide visibility.

**PASSIVE VULNERABILITY SCANNER**

SecurityCenter can make use of Tenable’s Passive Vulnerability Scanner (PVS) and treat the data collected as if it came from an active Nessus scanner or Intrusion Detection System. This means an organization can deploy a PVS (sometimes alongside or on their x86 based NIDS) and perform a majority of their vulnerability management without sending a single packet.

Although passive in nature, on a busy enterprise network a single PVS will typically return more data than a default Nessus scan. PVS will also accurately report any uncommon ports in use. For a Nessus scan to obtain similar results, it would need to scan all 65,535 ports to find any new malware, backdoors, management interfaces, and applications. The PVS also sees client side applications such as email, web browsers, and chat clients. All of this data can be used to perform dynamic asset discovery as well as rogue host detection.

PVS licenses are not included with SecurityCenter and must be procured separately.

**LOG CORRELATION ENGINE**

Tenable’s Log Correlation Engine (LCE) is a software module that aggregates, normalizes, correlates, and analyzes event log data from a wide variety of devices within the infrastructure. The LCE works identically with either SecurityCenter or the LCE Manager (event only) to provide an input of consolidated event data for analysis. Since the LCE is closely integrated with SecurityCenter, log analysis, IDS events, and vulnerability management can be centralized for a complete view of the security posture.

The LCE Clients are agents that are installed on systems whose logs, network traffic, performance, and other types of protocols and technologies are to be monitored by
forwarding data securely to the LCE server. Once a LCE server is installed and configured, one or more LCE clients can be used to send information back for normalization and correlation.

The LCE runs alongside other Tenable products (SecurityCenter 4 or greater) or separately and can handle a large number of events from firewalls, IDS devices, routers, honey-pots, servers, applications, and even SecurityCenter itself. LCE can collect events via syslog and can also make use of either a generic Linux or Windows agent that speaks a wide variety of protocols such as OPSEC and securely forwards events back to the LCE daemon. LCE also performs behavioral and event correlation and can send these alerts to SecurityCenter.

All SecurityCenter users with permission to see vulnerability or IDS traffic will be able to see LCE data if it is available. For example, a user who has access to the set of IP addresses comprising the “Microsoft Exchange Servers” would be able to see all vulnerabilities, IDS events, and logs for those systems.

The LCE can have a dramatic impact on the picture presented to SecurityCenter end-users. For example, LCE includes a “netflow” and “network sniffing” agent that can be used to log all network connections. Having this data at every user’s fingertips can cut down on the guesswork involved with troubleshooting, incident response as well as just trying to understand what is occurring on the network.

LCE licenses are not included with SecurityCenter and must be obtained separately.

**THIRD-PARTY DATA SOURCES (IDS EVENTS AND LOG SOURCES)**

The LCE supports syslog and SNMP trap analysis (IBM RealSecure and Proventia) of IDS events from a wide variety of sources. These IDS solutions need to be configured to send SNMP or syslog events directly to the LCE, which interprets and then forwards the data on to SecurityCenter.

For IDS signature updates, SecurityCenter is configured to directly access the Internet, support sites, or management consoles of the supported IDS solutions. Downloaded signatures are regularly pushed out to the LCE for IDS collection and correlation. This allows the LCE to build a current reference model of all the signature events checked for by the IDS it is monitoring logs from. The correlation is done by matching CVE (http://cve.mitre.org/) and BugTraq (http://www.securityfocus.com/bid) IDs with Nessus and PVS plugin information. This supports the high-speed vulnerability correlation process as well.

If one or more LCE servers are in use, then there are thousands of potential log sources that can be aggregated, normalized and correlated.

For more information about log correlation, consult the LCE documentation available at https://support.tenable.com/support-center/.

**SUPPORTED OPERATING SYSTEMS AND ENVIRONMENTS**

Tenable software supports a wide variety of operating system platforms and adapts well to nearly every enterprise environment. The table below provides a list of Tenable products and supported platforms:
<table>
<thead>
<tr>
<th>Tenable Product</th>
<th>Supported Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SecurityCenter</strong></td>
<td>Red Hat Linux ES 4, ES 5, and ES 6. CentOS 5 and 6</td>
</tr>
<tr>
<td><strong>LCE Manager</strong></td>
<td>Red Hat Linux ES 4, ES 5, and ES 6. CentOS 5 and 6</td>
</tr>
<tr>
<td><strong>Nessus 5</strong></td>
<td>Red Hat Linux ES 4, ES 5, and ES 6. CentOS 4, 5, and 6</td>
</tr>
<tr>
<td></td>
<td>Fedora Core 16</td>
</tr>
<tr>
<td></td>
<td>SUSE 10 and 11</td>
</tr>
<tr>
<td></td>
<td>Debian 6</td>
</tr>
<tr>
<td></td>
<td>FreeBSD 9</td>
</tr>
<tr>
<td></td>
<td>Ubuntu 8.04, 9.10, 10.04, 10.10, and 11.10</td>
</tr>
<tr>
<td></td>
<td>Mac OS X 10.6 and 10.7</td>
</tr>
<tr>
<td></td>
<td>Windows XP, Server 2003, Server 2008, Vista and 7</td>
</tr>
<tr>
<td><strong>Log Correlation Engine Server</strong></td>
<td>Red Hat Linux ES 4 (i386 only), ES 5, ES 6 (i386 and x86-64)</td>
</tr>
<tr>
<td><strong>LCE Clients</strong></td>
<td><strong>Log Agent</strong></td>
</tr>
<tr>
<td></td>
<td>Red Hat Linux ES 4, ES 5, ES 6 AIX 5.3</td>
</tr>
<tr>
<td></td>
<td>FreeBSD 7 and 8</td>
</tr>
<tr>
<td></td>
<td>Fedora Core 13-15</td>
</tr>
<tr>
<td></td>
<td>Solaris SPARC (8, 9, 10)</td>
</tr>
<tr>
<td></td>
<td>Ubuntu 8.xx-11.xx</td>
</tr>
<tr>
<td></td>
<td>Mac OS X</td>
</tr>
<tr>
<td></td>
<td>Dragon Appliance</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional, Server 2003, Server 2008, Vista and 7</td>
</tr>
<tr>
<td></td>
<td><strong>Tenable RDEP Monitor</strong></td>
</tr>
<tr>
<td></td>
<td>Red Hat Linux ES 4, ES 5, ES 6</td>
</tr>
<tr>
<td><strong>OPSEC Client</strong></td>
<td>Red Hat Linux ES 4, ES 5, ES 6</td>
</tr>
<tr>
<td><strong>Splunk Client</strong></td>
<td>Red Hat Linux ES 4, ES 5, ES 6</td>
</tr>
<tr>
<td><strong>Tenable Network Monitor</strong></td>
<td>Red Hat Linux ES 4, ES 5, ES 6 AIX 5.3</td>
</tr>
<tr>
<td></td>
<td>FreeBSD 7 and 8</td>
</tr>
<tr>
<td><strong>Tenable Netflow Monitor</strong></td>
<td>Red Hat Linux ES 5, ES 6</td>
</tr>
<tr>
<td></td>
<td>FreeBSD 7 and 8</td>
</tr>
<tr>
<td><strong>Passive Vulnerability Scanner</strong></td>
<td>Red Hat Linux ES 4, ES 5, ES 6</td>
</tr>
<tr>
<td></td>
<td>Windows Vista, Server 2008, and 7</td>
</tr>
</tbody>
</table>

**securityCenter Communications and Repositories**

The following table summarizes the components’ primary repositories and communication methods. For a visual depiction of the data flows, please refer to the diagram in [Appendix 1](#).
Table 2 – Repositories and Communication Methods

<table>
<thead>
<tr>
<th></th>
<th>SecurityCenter</th>
<th>LCE Manager</th>
<th>Nessus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Directory</td>
<td>/opt/sc4</td>
<td>/opt/sc4</td>
<td>Linux: /opt/nessus/ Windows: C:\Program Files\Tenable\Nessus</td>
</tr>
<tr>
<td>User Data</td>
<td>/opt/sc4/orgs/&lt;Organization Serial Number&gt;</td>
<td>/opt/sc4/orgs/1/</td>
<td></td>
</tr>
<tr>
<td>Repositories</td>
<td>/opt/sc4/repositories/&lt;Repository Number&gt;</td>
<td>/opt/sc4/repositories/1/</td>
<td></td>
</tr>
<tr>
<td>Audit Log</td>
<td>/opt/sc4/admin/logs/</td>
<td>/opt/sc4/admin/logs/</td>
<td></td>
</tr>
<tr>
<td>Organization Logs</td>
<td>/opt/sc4/orgs/&lt;Organization Number&gt;/logs/</td>
<td>/opt/sc4/orgs/1/logs/</td>
<td></td>
</tr>
<tr>
<td>Communication Interfaces</td>
<td>User Access: HTTPS</td>
<td>TASL Plugin Updates:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plugin Updates: Acquired over SSL from Tenable servers directly to SecurityCenter or for offline installation. Plugin packages are secured via 4096-bit RSA digital signatures.</td>
<td>Acquired over SSL from Tenable servers directly to SecurityCenter or for offline installation. Plugin packages are secured via 4096-bit RSA digital signatures.</td>
<td></td>
</tr>
<tr>
<td>User Data Repository</td>
<td>(optional if users have custom plugins): /opt/nessus/var/nessus/users/&lt;username&gt;/plugins/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Log Repository</td>
<td>Linux: /opt/nessus/var/nessus/logs/nessusd.messages</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows: C:\Program Files\Tenable\Nessus\logs\server.log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Interfaces</td>
<td>Communicates with SecurityCenter over SSL and uses SSL certificates for host verification to perform security scans, receive plugin updates and send scan results to SC. Uses a separate process (nessusd) per target for scanning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Correlation Engine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation Directory</td>
<td>/opt/lce</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Data Repository</td>
<td>/opt/lce/db</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Log Repository</td>
<td>/opt/lce/admin/logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Interfaces</td>
<td>With SecurityCenter: SSH and SCP over port 22</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alerts (optional): Sent to external syslog systems on UDP port 514 (syslog)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passive Vulnerability Scanner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation Directory</td>
<td>/opt/pvs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Data Repository</td>
<td>PRM files: /opt/pvs/var/pvs-proxy/scans</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PASL scripts: /opt/pvs/var/pvs-proxy/scans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Log Repository</td>
<td>Linux: /opt/pvs/var/pvs/logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Interfaces</td>
<td>Inbound Communications: Listens on TCP port 1243 (configurable) for inbound SC communications. Uses SSL key authentication, configured in the pvs-proxy.conf file. Plugin updates are over SSL.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outbound Communications (optional): Sends alerts via UDP port 514 (syslog).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ARCHITECTURE
SecurityCenter can be deployed in multiple architecture models, providing scalability from simple small networks to extremely large and complex ones. This is accomplished using one or more SecurityCenter servers in tandem with strategically placed scanners and LCEs.

VIRTUALIZED ENVIRONMENTS
SecurityCenter is well-suited to virtual platforms and comes prepackaged along with Nessus and PVS on the Tenable Appliance VMware image. Because of the unique performance considerations with virtualized platforms, please contact your VM software vendor for recommendations as VMs typically see up to 30% loss in efficiency compared with dedicated servers.

SINGLE SERVER ARCHITECTURE
For small networks (e.g., a few Class C networks or less than 1000 IPs), all of the vulnerability assessment components of SecurityCenter can be installed on a single server. The Tenable appliance, both virtual and hardware platforms, takes advantage of this ability. However, for optimal performance and to avoid potential resource contention, or in cases where single-server resources become overtaxed, Tenable recommends that PVS and Nessus be installed on separate servers from SecurityCenter. Deploying on separate servers is the recommended best practice when deploying into networks having over 1000 IP devices.

Due to resource issues, installing an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) on the SecurityCenter server is not supported.

When installed on a single server, the primary processes that will be running and active include nessusd (Nessus), pvs (PVS), pvs-proxy (PVS), Jobd (SC) and httpd (SC). These processes are “always-on”, while there are others that run “on demand” at various times.

The SecurityCenter RPM does not include Nessus, LCE, or PVS. They must be obtained and installed separately.

The Nessus server will be running the Nessus daemon on TCP port 8834. The server will also typically run the Apache web server on TCP port 443, as well as SSH on TCP port 22.
SecurityCenter, Nessus, and PVS installed on a single server

This configuration supports multiple organizations and can conduct and store scans for a fairly large group of users. It does not, however, take advantage of more than one Nessus scanner or PVS. In addition, it does not make use of the event processing or log management of the LCE.

Depending on the size of the scanned network, it may suffer performance problems while a scan is being conducted. For example, when no scans are occurring, the Apache web server uses a majority of the system resources to provide fast responses to user queries about the current network vulnerabilities. However, when a scan is occurring, the scan daemon will consume a noticeable amount of system resources. A dual CPU system will help, but placing the scan daemon(s) on a separate system is the best way to limit the impact to SecurityCenter.

The SecurityCenter server can include the LCE component as well; however, the additional processing involved with log correlation is ideally handled by a separate host.

All of the functionality of SecurityCenter is available, even though only one server is being used. Nessus network scans can be scheduled as often as desired, either with or without
credentials. One or more SecurityCenter users can be created, each with different roles and data access. Reports can be scheduled. The only functionality lost with a single server architecture is load balanced scanning or any type of scan that requires multiple scanners.

In this architecture, no matter how fast the CPU is, there will always be a noticeable difference in SecurityCenter responsiveness during scans.

Although each network is different, Tenable recommends at least 4 GB of system memory for this configuration.

SecurityCenter users employ their web browser to access their security information. These users can be within the network, coming across a VPN or anywhere else they have network access.

**MULTIPLE SCANNER ARCHITECTURE**

Expanding the above architecture, multiple Nessus and PVS systems can be added for each Class C subnet to be scanned. To add these devices to SecurityCenter, they should first be installed in their desired locations and then entered into the SecurityCenter configuration by the administrator.

In the diagram below, SecurityCenter is deployed on a server in the lower right and multiple Nessus scanners are deployed across the small network. The icons show four PVS systems deployed on various network segments.
In this configuration, when an active scan occurs, the targets are divided between the active scanners. During active scans, the CPU usage on the SecurityCenter server is very minimal. Console users will not see a difference in the vulnerabilities reported, but they will see much less network impact and their scans will complete several times faster than previous scans.

Vulnerability data from the PVS is handled differently. Since it is running 24x7, it is configured to record vulnerability data and make it available to SecurityCenter once an hour by default. SecurityCenter will save any passive vulnerability data for 7 days by default. Vulnerability data from a PVS automatically shows up in SecurityCenter and populates its knowledge of network vulnerabilities.

With this distributed architecture, the Nessus scanners can also be used to target networks other than what they scan for by default. In the network depicted above, each Nessus scanner would have been associated with their default target networks, which is called a “zone”. SecurityCenter scans can be configured to override default zones and ask, for example, the Nessus scanner in the upper portion of the network to scan the network segment on the bottom. This type of “zone” scanning allows for testing of firewall policies and exercising network IDS sensors.

When multiple Security Centers exist in an organization, each Nessus and PVS scanner can only be connected to one SecurityCenter at a time. If an individual Nessus or PVS scanner is connected to different SecurityCenters, plugins and reports will not be updated properly.
**SINGLE LOG CORRELATION ENGINE ARCHITECTURE**

SecurityCenter’s capabilities can be extended with one or more LCEs. This engine can be deployed either on the same or a separate server and can receive logs from many different devices including IDS/IPS devices. All logs are sent to the LCE and very little data is sent back to SecurityCenter.

A common strategy for Tenable Network Security customers is to upgrade a SecurityCenter with one LCE.

In the above network diagram, SecurityCenter and a single LCE are placed on two different servers.

Although not shown, dozens of LCE agents can be placed on key servers and at network choke points to aggregate as many logs as possible. The agents would connect back over TCP port 31300 to the LCE. Devices that can generate syslog messages can also be sent to the LCE. This syslog data can also include IDS data from a wide variety of intrusion detection devices. Other supported protocols include SDEE, RDEP, OPSEC, and SNMP.

SecurityCenter communicates with the LCE through secure SSH connections. All reporting and data analysis is presented through the SecurityCenter UI, but performed remotely by the LCE. If the LCE discovers an anomaly or a specific type of event correlation, it can send a message to SecurityCenter that treats the alert as if it came from an intrusion detection device.
SecurityCenter users can analyze any normalized log and correlated events obtained by the LCE with the same rights the user has to look at vulnerabilities. Users with the appropriate role-based permissions automatically have this access.

Below is an example screen capture of a port summary performed by the LCE while logged into SecurityCenter. In this case, the user has selected the “Port Summary” tool for all events in the past 24 hours.

![Port Summary](image)

**Example Port Summary listing of all LCE normalized logs**

**Multiple Log Correlation Engine Architecture**

SecurityCenter can make use of more than one LCE. Later in this section, we will discuss configuring SecurityCenter to make use of multiple “Organizations”, each of which is a collection of vulnerabilities, events and unique users. A single SecurityCenter can have as many Organizations as desired. Each Organization can also have one or more of its own LCEs.

From the SecurityCenter’s point of view, it really does not matter how each remote LCE is configured. One LCE could be focused completely on long-term NetFlow monitoring, another on firewall logs, and another on application logs from Exchange, the SQL farm and the Citrix server.

**Multiple SecurityCenter Architecture**

One of the benefits of SecurityCenter 4 is the ability to run multiple SecurityCenters in a distributed architecture where repositories of data can be shared securely between the individual SecurityCenters. This configuration gives flexibility to large enterprises that wish to monitor distributed environments and greatly enhances the aggregated reporting capability over a single SecurityCenter. This functionality is accomplished through the use of remote repositories.
In addition to network attached environments, repositories can be shared between discrete networks where one or both are detached from the network, such as SCADA or high-security networks. This functionality is accomplished using offline repositories.

**USER MANAGEMENT**

SecurityCenter implements a hierarchical access to data through the definition of Organizations and user roles. The Organizational repository, scan zone, and asset lists specify the IP address space that the defined users within the Organization have access to. Users are limited based on their role permissions and assigned resources. No SecurityCenter Organization or user can view data that they are not explicitly permitted to view. SecurityCenter can define and segregate user roles so that some audit users cannot see events, some can only see normalized events, and others can do unlimited log search. User access to LCE raw log data is configurable on a “per-LCE” basis.

Users with the “Manage Users” role (Manager users and the Organization Head by default) have control over users that they create and their subset of users. For example, consider the hierarchy below:

---

**Example Organizational Configuration**
In Organization A, the Org Head user has control over all Users and Managers in Organization A. Manager 1 similarly has control over all Managers and Users (except the Org Head user). Manager 2, however, only has control over Users B through G since User A and Manager 1 are not in their hierarchy.

In Organization B, Manager 3 has control over all Organizational users except for the Org Head user. We have created two users with custom roles. These custom roles have the “Manage Users” role and subsequently were able to create Users H through J. Custom 1 has control over Custom 2 along with all Users; however, Custom 2 only has control over Users I and J.

It is important to consider these concepts when working with the built-in roles and creating custom ones as they relate to your organizational structure.

**Organizational Security Model**

An “Organization” is defined as a set of distinct users. Organizations are assigned repositories and “zones” within one or more specified IP networks. Organizations can have overlapping repositories, and a single repository can be viewed and updated by multiple Organizations. In the diagram below, the “Compliance” repository shares vulnerability data collected from two different subnet ranges within the same company. Both Organization 1 and Organization 2 have access to this repository of data.
Sample Configuration with Multiple Organizations and Overlapping Repositories

Each network segment accessible by an Organization can be associated with specific Nessus daemons as a “scan zone”. SecurityCenter allows Organizations to be configured with two different scan zone modes: “selectable” and “forced”. If an Organization is in “selectable” mode, any available zones and their assigned scanners can be associated with the Organization and made available to users for scanning configuration. If an Organization is in “forced” mode, the selected zone will always be used for every scan performed by users in that organization.

When in “selectable” mode, at scan time, the zones associated with the Organization and a selection of “default” are available to the user. When a scan is configured to use a specific zone in either selectable or forced mode, the zone’s ranges are ignored and any IPs in the managed ranges for that user will be scanned by the Nessus scanners associated with the chosen zone.

When a scan is configured to use the “default” zone, the targets for the scan will be given to scanners in ALL zones in the application based on the zone’s specified ranges. This facilitates optimal scanning.
This configurability is very useful if an Organization is placed behind a firewall or NAT and has conflicting RFC1918 non-Internet-routable address space with another Organization. Some Organizations may benefit from the ability to override their default scanners with scanners from a different zone. This allows an Organization to more easily run internal and external vulnerability scans.

When setting up a zone, the ranges will be defined, such as 10.0.0.0/8, if the "default" zone is used, no scan outside of the 10.0.0.0/8 network would be permitted. However, it is quite common for large networks to contain multiple RFC1918 addressed networks that contain overlapping IP ranges. In this case, multiple zones could be specified with the appropriate scanner handling the desired range.

The SecurityCenter administrator can add an Organization’s network range as an IP address, a range of IP addresses or as a CIDR block. For example, 192.168.10.22, 192.168.10.22-192.168.10.24 as well as 192.168.10.0/24 are acceptable.

**Defining Single or Multiple Organizations**

SecurityCenter can be defined with either a single Organization or with multiple Organizations and access control roles can be used for users within one Organization.

For any type of SecurityCenter deployment that has logically distinct networks, it really does not make any sense to try to put these groups together in one set of users. For example, military networks often have a “Secret” network not connected to the “Unclassified” network. These different networks often have different audit, analysis, and reporting requirements. Similarly, a security consultant would not want to mix data from two or more Organizations in the same report.

However, if your users all have the same type of employee badge, it makes more sense to implement everyone with varying roles and resources as part of a single Organization. Within an Organization, there are many opportunities to differentiate users by what assets they can manage and resources they are assigned.

**Users and Roles**

SecurityCenter has various types of users defined by configurable roles, resource assignments and access levels. Users created by another user automatically inherit the roles and resources assigned to the user that created them. The following roles are defined within SecurityCenter:

- Administrator
- Organization Head
- Manager
- End User
- No Role

![Warning]

The Administrator, Organization Head, and No Role roles are fixed and may not be modified. Manager and End User roles are configurable.

An administrator is an account that has management responsibility over the console. By default, this account is named the “admin” account, although this can be changed to any
name and there can be multiple administrator accounts. The primary task of the administrator is to correctly install and configure Organizations. In addition, the administrator adds components, such as PVS, LCE, and Nessus, to the SecurityCenter to extend its capability. The administrator is automatically assigned the “Manage Application” role.

An Organization Head is the account within an Organization that has a broad range of security roles within the defined Organization. This is the initial user that is created when a new Organization is created and only one exists per Organization. They have the ability to launch scans, configure users (except for the administrator user) within their Organization, and define vulnerability policies and other objects belonging to their Organization. Each Organization has one **Organization Head** account that cannot be deleted. Permission-wise, the Organization Head user is nearly identical to the Manager user, however there are differences:

1. The Organization Head can add, edit, and delete roles, while the Manager cannot.
2. The Organization Head can add users that are the subordinate of any Manager or user with the “Manage Users” permission. The Manager can only add users as a subordinate of themselves.
3. The Organization Head has visibility of scan schedules and report definitions for the entire Organization, while the Manager can only see those of his/her subordinate.

Additional users can be created and assigned one of three possible predefined roles or a custom role. The predefined roles are “Manager”, “End User” and “No Role”.

The “Manager” role is intended for security team managers who have the need to manage users, vulnerabilities, resources and scans. The Manager user is very similar in capability to the Organization Head user except that they cannot manage roles and cannot manage objects not in their hierarchy (all Organizational users are in the Organization Head’s hierarchy).

An end-user could be an authorized system administrator, network/security engineer, or security auditor. They use their account to review security data, create and view reports, enter in their remediation actions to close tickets, and if given the proper credentials, launch scans.

“No Role” is the default “catch-all” role for users or objects for which no role has been assigned or explicit roles have been removed.

**User Visibility**

An important concept of SecurityCenter 4 is that of “Visibility”. Objects can have one of four possible visibilities.

The table below describes each of the available visibility options:

**Table 3 – Visibility Options**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Objects created with <strong>User</strong> visibility are available only to their creator.</td>
</tr>
</tbody>
</table>
**Organizational**

Objects created with “Organizational” visibility are available to any user within the current Organization.

**Application**

Objects created with “Application” visibility apply to any user within any Organization on SecurityCenter. Objects created by the administrator user automatically inherit “Application” visibility.

Only administrators can create objects with this visibility.

**Shared**

Objects created with “User” or “Organizational” visibility can be converted to “Shared” visibility after being shared by a user with the required permissions. If you edit an object that has a shared visibility, you have the option to change it to “User” visibility, which would remove all existing shares. In addition, if an object is unshared from everyone it reverts to user visibility.

**Access Control**

Within the defined user roles, granular permissions are defined that enable users to perform various tasks. Custom roles can be created with any combination of desired roles based on enterprise needs. Role permissions are broken down based on user visibility. In all cases except policy roles, an “Organizational” designation indicates that the user with that role can create objects with either “User” or “Organizational” visibility. In the case of scan policy creation, users with the “Create Policies” permission can only create policies with “User” visibility. Users with “Create Organizational Policies” and “Create Policies” permissions can create policies with either “User” or “Organizational” visibility. Users with only the “Create Organizational Policies” permission cannot create any scan policies.

The table below defines the various default permissions available within the SecurityCenter architecture:

**Table 4 – Available Permissions**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
<th>Organization Head</th>
<th>Administrator</th>
<th>Manager</th>
<th>End User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept Risks</td>
<td>Accept the risk of vulnerabilities</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Alerts</td>
<td>Create custom alerts</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Create Audit Files</td>
<td>Upload custom audit files</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Copyright © 2002-2012 Tenable Network Security, Inc.
<table>
<thead>
<tr>
<th>Create Application Roles</th>
<th>Create roles with application visibility. This is not a configurable role.</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Organization Roles</td>
<td>Create roles with Organizational visibility. This is not a configurable role.</td>
<td>X</td>
</tr>
<tr>
<td>Create Organization Assets</td>
<td>Create assets</td>
<td>X X X</td>
</tr>
<tr>
<td>Create Organization Credentials</td>
<td>Create credentials</td>
<td>X X X</td>
</tr>
<tr>
<td>Create Organization Policies</td>
<td>Create scan policies with Organizational visibility. This option must be used in conjunction with the “Create Policies” permission.</td>
<td>X X X</td>
</tr>
<tr>
<td>Create Organization Queries</td>
<td>Create queries</td>
<td>X X X</td>
</tr>
<tr>
<td>Create Policies</td>
<td>Create scan policies with “User” visibility.</td>
<td>X X X</td>
</tr>
<tr>
<td></td>
<td>This option must be set for the “Create Organizational Policies” option to function.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use this option for users who will create policies for themselves, but not shared policies. This can be useful for new users.</td>
<td></td>
</tr>
<tr>
<td>Create Tickets</td>
<td>Create tickets</td>
<td>X X X</td>
</tr>
<tr>
<td>Edit/Delete Organization Assets</td>
<td>Edit or delete assets belonging to the user’s Organization regardless of what Organizational user created it.</td>
<td>X</td>
</tr>
<tr>
<td>Edit/Delete Organization Credentials</td>
<td>Edit or delete credentials belonging to the user’s Organization regardless of what Organizational user created it.</td>
<td>X</td>
</tr>
<tr>
<td>Edit/Delete Organization Policy</td>
<td>Edit or delete policies belonging to the user’s Organization regardless of what Organizational user created it.</td>
<td>X</td>
</tr>
<tr>
<td>Edit/Delete Organization Query</td>
<td>Edit or delete queries belonging to the user’s Organization regardless of</td>
<td>X</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Permissions</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Manage Applications</td>
<td>Manage SecurityCenter applications and services. Any role with the “Manage Applications” permission is non-editable. The permission column is removed.</td>
<td>X</td>
</tr>
<tr>
<td>Manage Users</td>
<td>Manage non-administrative users.</td>
<td>X X</td>
</tr>
<tr>
<td>Purge Tickets</td>
<td>Purge tickets</td>
<td>X X</td>
</tr>
<tr>
<td>Recast Risk</td>
<td>Recast the risk of vulnerabilities.</td>
<td>X X</td>
</tr>
<tr>
<td>Scan Privileges</td>
<td>Perform Nessus scans.</td>
<td>X X X</td>
</tr>
<tr>
<td>Share Assets</td>
<td>Share assets with other users.</td>
<td>X X X</td>
</tr>
<tr>
<td>Share Credentials</td>
<td>Share credentials with other users.</td>
<td>X X X</td>
</tr>
<tr>
<td>Share Dashboard Tabs</td>
<td>Share dashboard tabs with other users.</td>
<td>X X X</td>
</tr>
<tr>
<td>Share Policies</td>
<td>Share policies with other users.</td>
<td>X X X</td>
</tr>
<tr>
<td>Share Queries</td>
<td>Share queries with other users.</td>
<td>X X X</td>
</tr>
<tr>
<td>Update Plugins</td>
<td>Update Active, Passive and Custom plugins.</td>
<td>X X X</td>
</tr>
<tr>
<td>Upload Nessus Scan Results</td>
<td>Upload Nessus scan results.</td>
<td>X X X</td>
</tr>
<tr>
<td>View Event Data</td>
<td>View event data.</td>
<td>X X X</td>
</tr>
<tr>
<td>View Organization Logs</td>
<td>View Organization logs.</td>
<td>X</td>
</tr>
<tr>
<td>View Raw Logs</td>
<td>View raw logs.</td>
<td>X X X</td>
</tr>
<tr>
<td>View Vulnerability Data</td>
<td>View vulnerabilities within the Organizational repository.</td>
<td>X X X</td>
</tr>
</tbody>
</table>

**ASSET MANAGEMENT**

The IT and network management market is full of “asset management” and “asset tracking” solutions. Each has their own take on efficient accounting of configuration, inventory and roles, and each of these systems has their own advantages and scalability issues. What is good for managing several hundred Cisco routers may not be good for managing thousands...
of mobile laptops. Many asset systems also do not account for rapid network changes and quickly become outdated.

**Asset Definition**

The concept of “assets” depends on your point of view. A senior manager may view a Human Resources implementation of PeopleSoft as an asset, but not realize that it is made up of many different components. Similarly, a database administrator may see no technical difference between running Oracle on the payment systems or Oracle on the server tracking marketing data.

From a network management point of view, there are also many different systems, often with conflicting counts and information, that can produce lists of routers, types of servers, system owners and more.

**SecurityCenter Assets**

Tenable has implemented a flexible dynamic asset discovery system that can also import static asset lists from many commercial and open source systems. This allows “high level” asset lists to be constructed, as well as very detailed lists of specific items.

To upload a static list to SecurityCenter, a security manager would simply need to put the data into a text file that contains IP addresses, ranges of IP addresses, or CIDR notation. Once uploaded, the asset list is named and can be immediately used.

SecurityCenter can implement rules (entered through a wizard) that consider “discovered” information for dynamic asset discovery. These rules are run against vulnerability data and result in assigning an IP address to one or more asset lists. For example, SecurityCenter could create a rule that said any Windows systems that belonged to the “CORPORATE-NY” domain be placed on an asset list named “New York Domain”.

Tenable also utilizes a special asset-list type known as “Watchlists” for hosts outside of the normal protected zone. These assets are helpful with setting up queries and filters based on hosts outside of your repositories, such as blacklisted hosts and known attack vectors.

**Assets in Use**

All activities on SecurityCenter are controlled or influenced by dynamic and static asset lists.

- Users will have access to one or more asset lists.
- Users will only be able to see vulnerabilities, IDS events, and logs for their asset lists.
- Active scans can only be launched at hosts within a set of available asset lists.
- Reports will be performed against one or more asset lists.
- Tickets can be opened or closed for entire asset classes.
ABOUT TENABLE NETWORK SECURITY

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable’s award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com
APPENDIX 1: TENABLE DATA FLOW DIAGRAM

Tenable Unified Security Monitoring Architecture Overview