



**ProductivIT:
Security and Availability**



© 1999 - 2004 DynTek. All Rights Reserved.
Confidential Property of DynTek
18881 Von Karman Avenue. Suite 250. Irvine, CA. 92612

Introduction

The ProductivIT™ hosted application service is based on an operational framework that incorporates industry best practices for managed security and availability. The goal of the framework is to achieve mission-critical system integrity, reliability and availability. The framework specifies the processes necessary to manage a defined level of security and availability, including procedures necessary to respond to security and availability issues.

Basic Security Requirements

The following are fundamental requirements of the system related to security:

- ? Access control: Control over access to the application, its functionality and the data, is governed by user ID and password.
- ? Privacy: All communication between the application client and the hosted application service travels through an encrypted channel (1024-bit SSL). This helps ensure that data is viewable only to users with authorized access.
- ? Integrity: The secure channel helps to ensure that data traveling between the user and the application service is not altered by anyone other than the user.
- ? Auditing: All communication and operations on the hosted application service are logged and periodically monitored for performance and intrusion detection.
- ? Availability: A high level of availability for the hosted application is achieved through fault-tolerant design incorporating redundancy in all system components from physical to application level. System components are also continuously monitored to help maintain application availability through usage growth and to avert possible denial of service (DOS) attacks.

External Customer Requirements and Policies

ProductivIT will work with the customer to integrate specific customer security requirements or policies into the operational framework. For example, this may include

- ? Modification of automated notification procedures in the event of security or availability issues
- ? Requiring client-certificate based authentication to limit access to the application to specific workstations

-
- ? Configuring the hosted application service to run over a VPN or a dedicated private network

Security and Availability Design Features

All system components of the ProductivIT hosted application service, including Internet connections, routers, firewalls, and switches are fully redundant, providing both load balancing and failover capabilities. Firewall services are distributed through multiple independent points throughout the system, using dedicated appliances (SonicWall, Cisco PIX), with screening and logging of both in and out bound activity. All components are configured on the basis of the most current security information available, with adherence to a fundamental policy of default to denial – whatever communication is not expressly permitted is denied, and whatever process is not necessary is not running. Figure 1 shows a high-level view of the hosted application service infrastructure.

Security and Availability Procedures

Control of Administration and Maintenance of Data Center

Physical access to the data center and application service is restricted to only those personnel required to perform administrative tasks on the servers or network infrastructure. Physical access is restricted to only the screened personnel that are issued the following:

- photographic ID
- magnetic keycards
- traditional keys

All three items are required to obtain physical access to the ProductivIT servers. Physical access to the servers is logged and audited. Logical access to the ProductivIT servers and data is further restricted to the subset of personnel who have physical access and also have the necessary user account credentials to log on to the servers. Logical access to the servers is also logged and audited. A written application for physical and logical access must be approved and is logged.

Tracking and Auditing

All access to components constituting the ProductivIT hosted application service (network connectivity, servers, storage and server application) is monitored on a periodic basis to spot existing or impending problems. Traffic patterns and logs are reviewed and checked against known hacking exploit patterns, both by real-time automated monitoring

systems and by manual review on a daily basis. Current reference information is kept up to date through automated notification services from sources including Microsoft, CERT, and BugTraq, as well as continuous review of on-line security sites.

Application access is also recorded and reviewed, and summary reports listing usage time by user are available to the customer for statistics or investigation of potential misuse. Confirmed security incidents will be reported immediately to the client, and an appropriate level of response will be pursued together with them, ranging from a simple lockout of the offender to notification of legal authorities.

Performance Monitoring

System performance as defined by server and network utilization is monitored continuously, on 24x7 basis using IBM's Tivoli application management framework, as well as customized software monitoring tools. Metrics for server performance include CPU utilization, memory IO, and disk throughput. Metrics for network utilization include bandwidth usage by service and by customer. This data is evaluated to verify that system capacity exceeds utilization by a minimum of a factor of two, helping to ensure that enough overhead is available for usage spikes or potential denial of service (DOS) attacks. Should utilization exceed the threshold for any reason, capacity can be quickly increased through a number of means including

- ? addition of warm stand-by equipment
- ? fail-over to alternate data centers
- ? restriction of communications from offending clients (i.e. hackers)

Independent Review

ProductivIT engages external agencies to perform periodic security evaluations including external penetration tests. Internal security audits are also performed periodically, to insure that documented operational procedures are being followed. The results of the internal and external audits are used to determine the need for immediate changes, and to ensure that the long-term security and availability strategy will meet requirements. Should any changes to the application or service infrastructure be required, the modifications (source code, configuration files, network modifications) are reviewed by a security team independent of the application development team for compliance with standards.

ProductivIT Hosted Application Service Infrastructure

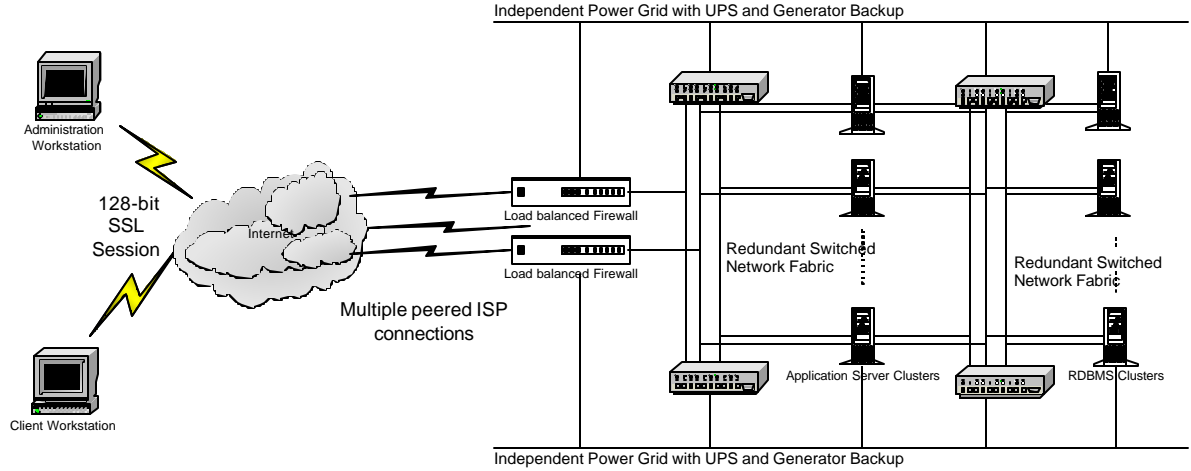


Figure 1