SUN MICROSYSTEMS | TELECOMMUNICATIONS

Sun microsystems

PROVISIONING OUTSOURCED UBIQUITOUS ACCESS

How Internet Service Providers can Create Business Opportunities with Sun's i-Planet™ Software

Provisioning Outsourced Ubiquitous Access

How Internet Service Providers can Create Business Opportunities with Sun's i-Planet™ Software

A White Paper by Sun Telco

Contributions by:
Bruce Baikie
Steve Gaede
Kevin Kalajan
Michael Wallace

Sun microsystems®

The products described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

THIS PUBLICATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. SUN MICROSYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

Sun microsystems

Contents

1. **Introduction** **1**

Changing the Parameters 2

The ISP Outsourcing Model 3

2. **i-Planet Product Overview** **5**

Remote Access Features 5

Outsourcing Resource Access 10

Administration 10

System Architecture 11

Gateway 11

Server 12

3. **Deploying i-Planet Software** **15**

Enterprise Configuration 16

Gateway Configuration 16

Server Configuration 18

ISP Configuration 18

Technical Considerations 20

Security 20

Performance 21

Scalability 21

Reliability 22

Ease of Administration 23

ISP Value-Added Services 24

4. Getting Started 25

5. References 27

Introduction 1

Organizations everywhere know the importance of leveraging their Information Technology (IT) infrastructure to increase productivity and enhance competitiveness. Armed with secure remote access to facilities like electronic mail and sophisticated ERP systems, employees, customers, consultants, partners, and suppliers become empowered to conduct business in new ways, around the world and around the clock. Travelling employees can access online information and respond to electronic mail as if they were in the office. Small field offices can be deployed close to customer locations with the same access to IT resources as they have from the main office. Companies can reap the benefits of allowing employees to telecommute with access to main office computing facilities. And they can foster closer, more effective relationships with consultants, partners, and suppliers by enabling direct access to specific services like supply chain management software.

Providing secure, ubiquitous remote access to employees, consultants, partners, and suppliers can be a daunting prospect — a costly and risky burden for large corporations, and prohibitively expensive for small ones. It is costly to deploy modem pools, pay for long-distance access, and to support, maintain, and upgrade software on employees' laptops and home computers. For small field offices, leased-line access comes at a premium, as does the installation and maintenance of customer-premises equipment at remote sites. Outlays become astronomical when an IT point-of-presence must be established at sales offices and suppliers overseas — one U.S. garment manufacturer estimates the expense to bring a new supplier online in Pacific rim countries at USD $500,000! Even at this price, the resulting infrastructure still cannot enable a company's sales force to quickly check product availability from a customer site.

Changing the Parameters

The advent of i-Planet™ software from Sun Microsystems changes the fundamental parameters by which companies provide access to internal systems — enabling secure, ubiquitous access that is dramatically less expensive than current techniques. Rather than providing access through low-speed modem banks or costly leased lines, i-Planet software leverages the ubiquitous nature of the Internet to provide safe access from anywhere that a Web browser is available. This enables organizations to employ the faster Internet connectivity available through cable modems, DSL, ISDN, and even through high-speed Internet connections at customer sites. Unlike solutions that are based upon Virtual Private Network (VPN) technology, i-Planet software supports connectivity from anywhere an authorized user might require access — including airport kiosks, Internet-enabled hotels, trade shows, and customers' offices.

Sun's i-Planet product provides authenticated users with the ability to access virtually any IT services for which they have been authorized, including electronic mail, calendering, internal Web sites, file servers, legacy systems with 3270 or 5250 emulator access — even applications running in the X Window System environment and Microsoft Windows 95, 98, and NT. Given i-Planet software's ability to interface to such a wide range of platforms, organizations can use it internally to provide universal application access regardless of the desktop platform. And because Sun's approach is server-based, all that is required on the client side is a Secure Sockets Layer (SSL)-enabled Web browser, like Netscape™ Communicator, saving the expense of configuring, maintaining, and upgrading client applications or VPN software.

The thin-client approach, known for its low cost of ownership, has many advantages when used to provide remote access. Because only a Web browser is required, laptops and home computers are no longer costly extensions of an organization's IT infrastructure that require complex configuration, support staff, and upgrades. No longer must a company's proprietary e-mail and sensitive files reside on laptops which are subject to loss or theft. With i-Planet software, replacement is fast and easy because only the client Web browser must be configured.

Rather than spending USD $500,000 on infrastructure, configuration, and leased lines, an extranet presence at an overseas supplier site can now be brought online with a local Internet Service Provider (ISP) account and a Web browser.

The ISP Outsourcing Model

Providing IT access to employees, telecommuters, partners, customers, and suppliers creates a unique opportunity for Internet Service Providers (ISPs). Organizations of all sizes recognize that effective and innovative remote access is a competitive edge. While larger companies typically invest in capital and staff to provide remote-access services, small- and medium-sized companies are also realizing the need to have the same world-class remote-access facilities.

To reduce costs, many small- and medium-sized companies choose to focus on their core business by outsourcing parts of their IT infrastructure, leaving the burden of capital investment, maintenance costs, upgrades, staff retention and training, and 24-by-7 availability to service providers. Sophisticated and expensive business applications are quickly becoming available to smaller companies on a subscription basis. With a 20-30 percent savings over internal costs, ISPs are unburdening overworked IT staffs by managing their customers' corporate messaging servers. And since the IT staffs at those small- and medium-sized companies already procure their Internet connectivity from ISPs, they have more incentive to outsource their remote-access requirements.

Sun's i-Planet software has an extremely broad set of capabilities, and is highly-customizable, making it an excellent outsourcing candidate for experienced service providers. The reasons for ISPs to provide such services for their customers include:

- Expert maintenance of a conventional modem pool, and faster access where direct Internet connectivity is available
- The ability to integrate worldwide Internet access for international remote access to companies of all sizes
- The market differentiation that results from providing a more comprehensive set of packaged services to customers
- A rapid sales cycle because installation and configuration of client software and hardware is not required

- The ability for ISP staff to provide extranet facilities without visiting or configuring routers and VPN devices in remote locations
- Ease of configuring field offices over the Internet
- A detailed transport-layer log that enables billing by use rather than by connect time.

The additional value found in Sun's i-Planet product is another compelling reason to take advantage of the remote-access service provisioning opportunity. Because of the wide range of configurable options available with i-Planet software, the first ISPs to market will be able to market a high degree of expertise which will help them to retain customers and differentiate themselves from the competition.

Of course, the i-Planet product is supported by the software already preferred by Internet Service Providers worldwide: the Solaris Operating Environment™ running on UltraSPARC™ processor-based servers from Sun Microsystems. Beginning with the server that comes with a PC price — the single-processor Ultra™ 5S server — ISPs can scale up the product line with expandable Ultra 10S systems. Where higher levels of CPU power are required, ISPs can enter the realm of Sun's highly-reliable multiprocessor servers beginning with the dual-processor Sun Enterprise™ 250 server, the quad-processor Enterprise 450 server, and all the way up to the 64-processor Sun Enterprise 10000 (Starfire™) server — with binary compatibility across the entire product line. For telephone company ISPs with even more rigorous environmental requirements, Sun's Netra™ t servers provide carrier-grade reliability in a NEBS Level-3 certified package.

The most cost-effective use of computing resources is of critical importance to ISPs, which is why Sun has prepared this white paper. It provides an overview of the capabilities of i-Planet software, and it demonstrates how ISPs can leverage its capabilities through configurations installed at customer sites, and with servers co-located at the ISP facilities. Regardless of configuration choice, the strong need for secure remote access will compel business customers to choose those ISPs providing i-Planet remote access services.

i-Planet Product Overview 2

Sun's i-Planet product provides remote and travelling employees with Internet-based access to a company's corporate network from any device with a Web browser. It acts as a mediator between authorized users and internal resources, providing secure remote user connectivity regardless of location with a uniform, familiar Web browser interface. Because it acts as a mediator with integrated firewall software, it can actually make corporate intranets more secure while simultaneously controlling access from remote users.

Remote Access Features

In a typical corporate environment, i-Planet software is deployed on two systems: a gateway and a server (Figure 1). The gateway is positioned between remote users and the corporate intranet. It contains an internal firewall, encryption platform, and a reverse proxy for incoming traffic. The server provides the initial Web pages viewed by users, authentication mechanisms, and access to applications on the corporate intranet. Together, the i-Planet technology gateway and server enable access to a wide range of services:

- *Authentication*

  The first activity when accessing i-Planet services is user authentication. This ensures that Internet-based remote access is secure. User authentication is handled over an encrypted SSL channel between the client Web browser and the i-Planet gateway. The gateway acts as a proxy to existing authentication mechanisms, eliminating the need to populate and synchronize multiple authentication repositories. i-Planet software integrates with the following standard methods, and can be extended to interoperate with other customer-specific mechanisms:

- RADIUS
- Microsoft Windows NT Domain
- Solaris™ NIS
- UNIX® Login and Password
- Safeword digital tokens from Secure Computing
- SecurID digital token from Security Dynamics
- S/Key single-use passwords developed by Bellcore
- API for customer-specific authentication (e.g., LDAP)

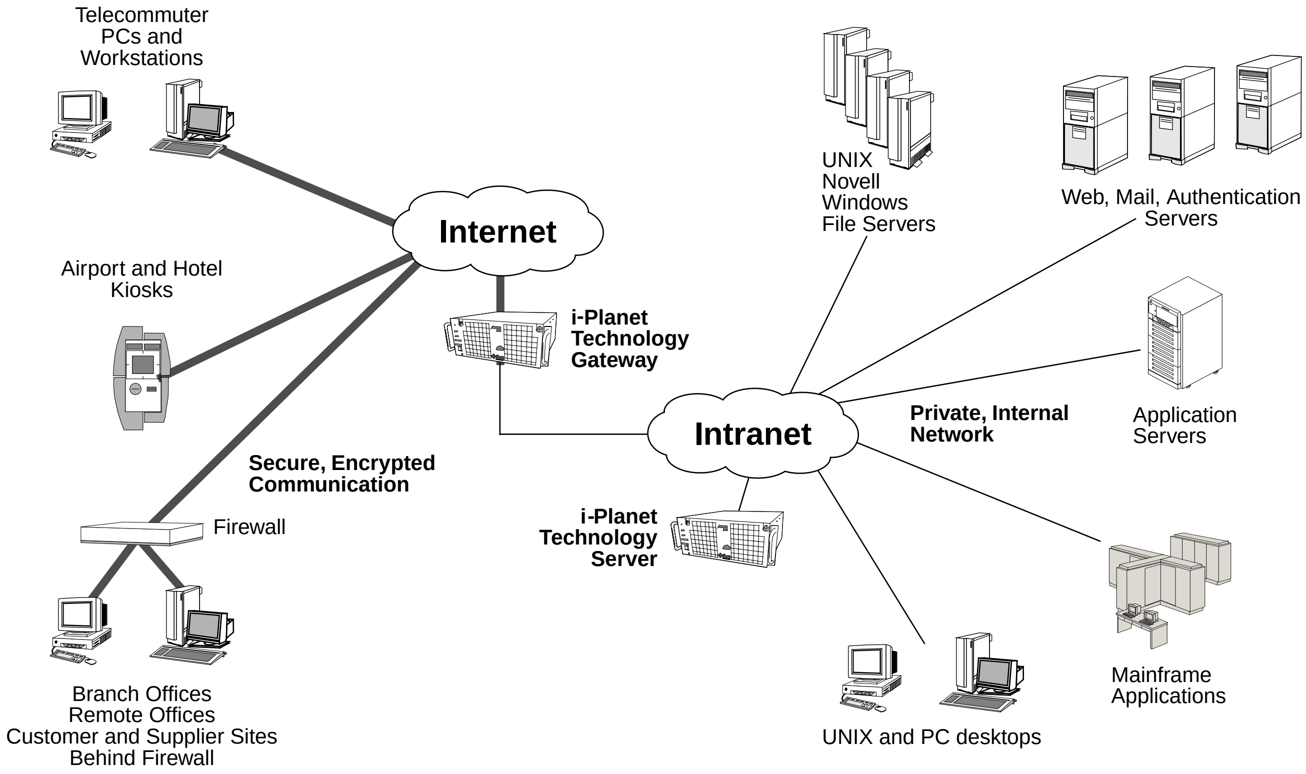
Telecommuter PCs and Workstations
Airport and Hotel Kiosks
Internet
i-Planet Technology Gateway
Secure, Encrypted Communication
Firewall
Branch Offices
Remote Offices
Customer and Supplier Sites
Behind Firewall
UNIX
Novell
Windows
File Servers
Web, Mail, Authentication Servers
Intranet
Private, Internal Network
Application Servers
i-Planet Technology Server
Mainframe Applications
UNIX and PC desktops

Figure 1 Secure, remote user access is provided by i-Planet software hosted on a gateway and a server platform. Remote users may be located anywhere on the Internet, including behind other corporate firewalls.

- *The i-Planet Desktop*

  The desktop is a Web-based user interface that is customized by each user's profile and by the administrator. It provides a central access point for other applications and information sources from the company. Once authenticated, the desktop is the first page viewed by the remote user.

- *Electronic Mail*

  Sun's i-Planet product provides four ways for users to access electronic mail that resides on the company's internal IMAP and SMTP servers.

  - The simplest user interface is written in pure HTML, making e-mail accessible on virtually any Web browser, even those not enabled with a Java™ virtual machine.
  - More sophisticated is the NetMail interface, which enables e-mail access through a Java applet which is downloaded to the user's Web browser. Most i-Planet software users prefer the NetMail interface because of its rich feature set, including disconnected e-mail reading.
  - To use HTML-based mail interfaces like those available with Microsoft Exchange or Lotus Notes, a connection to the appropriate server is made in the same way in which any internal Web server is accessed — except that, with i-Planet software, the Internet communication is authenticated and secure.
  - For those wishing to use client-based, third-party e-mail packages like Eudora or Microsoft Outlook Express, Sun's Netlet technology can be configured to proxy requests for any TCP/IP-based protocol from the remote system by multiplexing ports on the same encrypted connection to the i-Planet gateway system (Figure 2).

  One of the more powerful components of the i-Planet package, Netlet software is securely configured on the server side and downloaded to the user's Web browser as a Java technology applet, where it listens on the specified ports and securely tunnels requests back to the enterprise. Users need not configure complex VPN software, and all configuration choices (including which services to enable) are centrally-maintained. To use remote enterprise resources, users specify 'localhost' as the application's server, and Netlet technology does the rest.

- *Internal Web Site Access*

  Access to internal Web sites is enabled through the reverse proxy and the URL re-writer that reside on the i-Planet gateway system. These mechanisms check session validity, forward HTTP requests to the appropriate internal servers, and re-write URLs in the HTML that is provided back to the user. The URL re-writing mechanism can be used to enable access to HTML-based front-ends for applications that are not hardened for Internet access. The servers for these applications could not otherwise be made accessible without placing them in the company's DMZ — a move that would significantly endanger company security.

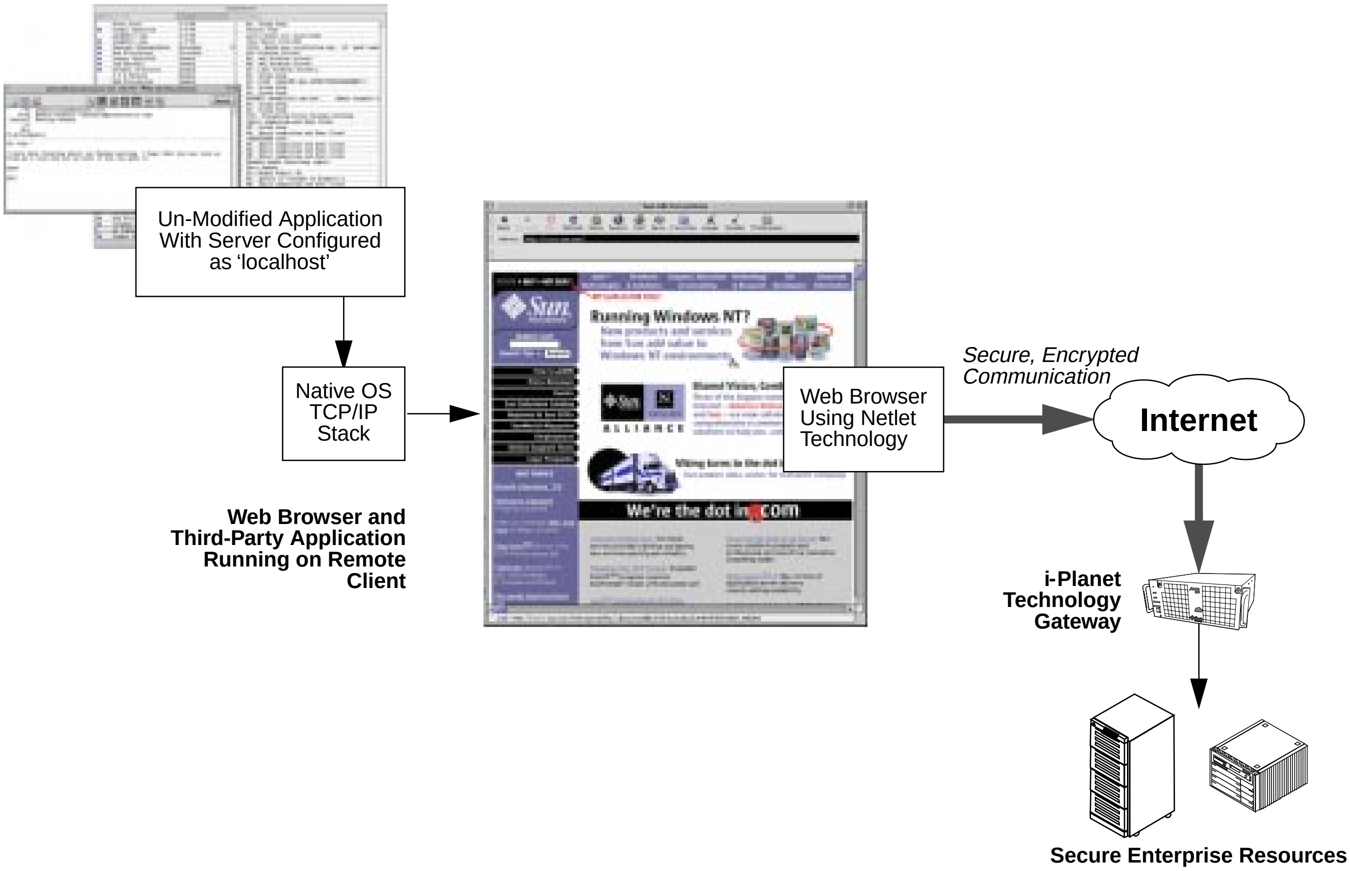
Un-Modified Application With Server Configured as 'localhost'
Native OS TCP/IP Stack
Web Browser and Third-Party Application Running on Remote Client
Running Windows NT?
We're the dot in .com
Web Browser Using Netlet Technology
Secure, Encrypted Communication
Internet
i-Planet Technology Gateway
Secure Enterprise Resources

Figure 2 The Netlet, one of the more powerful components of the i-Planet product, enables secure, encrypted communication from un-modified client applications back to servers in the enterprise network.

- *Calendaring and Scheduling*

  i-Planet software provides an HTML interface to Sun's CDE calendar and to the Sun Calendar Server. Other calendaring services like those supplied with Lotus Notes and Microsoft Exchange can be accessed using their HTML interfaces in the same way as any other internal Web site is accessed.

- *File Access*

  Users have browser-based, private file access to all authorized data files from any internal file server, whether via NFS™, SMB-based Microsoft Windows 95, 98, and NT, Novell, or even internal FTP servers. Given a file selection, the user's Web browser can be directed to start a helper application or to save the file on the client system. The i-Planet server makes downloading and uploading of files quicker and easier by compressing files before moving them across the Internet — resulting in fast response times.

  To further enhance performance, the i-Planet product's file management application supports recursive directory searches on the server, eliminating the constant network traffic that would be necessary if the search were performed by browser-resident software. In addition, the file manager can be used to attach files to e-mail messages on the server — eliminating the need to download files to the client system, make the attachments locally, and then upload the same files once attached to an e-mail message.

- *X Window System and PC Application Access*

  Sun's i-Planet software enables users to run existing PC or X Window System-based applications without changes. Using Netlet technology, Internet users can have access to remote control applications like Symantec's pcANYWHERE for managing their desktop PCs while away from the office. For X Window System-based applications, GraphOn's Go-Joe remote control software can be securely accessed via centrally-configured Netlet software. And for Microsoft Windows NT systems, inclusion of the Java technology-based Citrix ICA® client enables remote, platform-independent use of Microsoft Windows NT applications. In fact, given i-Planet software's ability to provide platform-independent access to such a wide variety of applications, there is merit to using it on internal networks so that one Web browser-enabled desktop system can access all enterprise applications.

- *Terminal Emulation*

  For access to ASCII interfaces on the internal network, i-Planet software uses a Netlet to support telnet sessions from remote users' Web browsers to systems on the company's internal network. Using Netlet technology, users can access 3270 or 5250 emulation provided with Netscape Communicator or with a Java technology applet.

Outsourcing Resource Access

With such a comprehensive set of capabilities available through Sun's i-Planet product, it takes users time to become acquainted with all of the powerful remote access tools they have at their disposal. Sun's experience is that the majority of users begin by accessing e-mail, and only some users perform complex activities like remotely managing their desktop systems and delivering presentations from software on their office desktops.

Internet Service Providers should consider the learning curve that users follow in becoming familiar with i-Planet software tools. In doing so, ISPs might focus first on providing a core set of remote access facilities, and later provide options to graduate to more complex value-added features.

Administration

The i-Planet product includes a Web browser interface to administration features. This administration console enables the management of all of the i-Planet servers, including:

- Adding, deleting, and managing user authentication mechanisms, policies, and roles
- Backing up and restoring configuration data
- Log administration
- Adding, deleting, and managing new services and applications
- Customization of the home page that users see when first authenticated

The i-Planet product's detailed logging and reporting information can enable service providers to bill customers based on more complex criteria than simply connect time, including volume of data transferred and number of functions executed. The log data includes:

- Data on each successful access, including user name, IP address, and duration of connection
- Data on all failed access attempts

System Architecture

Sun's i-Planet software runs on UltraSPARC processor-based servers running Solaris 2.6 or Solaris 7 operating software. The software is partitioned into two main components: a gateway and a server. Although it is possible to install both components on a single server — and the security implications of doing so are minimal — Sun recommends running the gateway and server packages on separate systems.

Gateway

The gateway establishes the boundary between the Internet and a company's internal network. Everything on the Internet side is considered insecure, and everything on the internal side is considered secure. The gateway has one network interface to the Internet and one interface to the internal network. The gateway includes the following components:

- *SunScreen™ Security Technology*

  The gateway can be fortified with the optional firewall package, which is built using the same dynamic packet-filtering software that is provided with SunScreen™ EFS security software. The firewall ensures that the gateway can be accessed from the Internet only using the SSL port, and it inspects each packet in a session to ensure that none are inserted by an intruder.

- *Encryption Technology*

  The gateway contains an implementation of the Secure Socket Layer (SSL) that uses self-generated certificates. This SSL package handles encryption for all SSL conversations with the remote user's Web browser. In addition, multiplexed communication between the browser's Netlet and the gateway is encrypted using the more high-efficiency RC5 algorithm. With all communication to the Internet encrypted and decrypted, the deployment of the gateway on a separate server ensures that sufficient computing power is available to handle potentially heavy workloads.

- *Reverse Proxy*

  The reverse proxy acts as an intermediary between a variety of different service requests and the internal systems which can satisfy them. The reverse proxy ensures that no packet traverses the gateway without being inspected and potentially re-written to address the correct server.

- *URL Re-Writer*

  The URL re-writer acts like the reverse proxy except in the HTTP domain; it re-writes requests to internal services so that they address the intended server, and it re-writes URLs on the responses so that subsequent requests can be properly interpreted by the gateway.

- *EPROX*

  EPROX is the software which manages the gateway end of communications with the browser-based Netlet software. EPROX de-multiplexes all of the multiple simultaneous connections (for example, remote control or telnet) that might be managed over the single encrypted connection with the remote user’s browser.

Server

The i-Planet technology server handles all of the details of authorization, authentication, policy, user profile access and management, and baseline remote access functionality. The individual components of the server work together and interface with external data sources — for example RADIUS authentication — to manage the process of identifying users to the system, determining access rights, and providing that access. The primary components of the server are independently linked, so that many different technologies can be integrated without making major changes. The server consists of several subsystems.

- *Authentication*

  The authentication subsystem authenticates users based on internally-generated challenge-response mechanisms like S/Key single-use passwords, or it integrates with existing mechanisms like RADIUS, NIS, and token-based systems like SecurID and Safeword.

- *Authorization*

  This mechanism determines access rights for the remote user based on the username supplied by the authentication subsystem, and the resources and rules from the policy manager.

- *Policy Manager*

  The policy manager handles the relationships between policies, resources, and users.

- *Profile Manager*

  This subsystem stores application and user profiles and interfaces with external data sources such as files and directory servers. Application and user profiles determine the allowable set of roles that can be filled by the authenticated user. The profiles also contain additional user-specific application and personal information.

- *Application Services*

  This component consists of a core set of applications that enable remote access functionality, including e-mail, calendaring, and file access. Application services, for example, is where compression of remotely-accessed files occurs.

With the functions of the i-Planet technology gateway and server systems outlined, the issue of how ISPs can best deploy them is explored next.

Deploying i-Planet Software 3

There are two ways in which service providers can leverage i-Planet software to meet the remote access needs of their business customers:

- *Enterprise Configuration*

  Many ISPs already provide their business customers with value-added services, including on-site support of routers and firewalls. The enterprise configuration of the i-Planet product involves installing and maintaining both the gateway and server at the customer site. This enables ISPs to offer an increasingly wide range of services to customers, however this model does not provide the leverage and economy of scale of the ISP configuration.

- *ISP Configuration*

  A growing number of companies outsource IT functions to let them focus on their core business issues. In this model, ISPs do what they do best, and their business customers avoid the pitfalls of hiring, training, and retaining skilled IT personnel. Many ISPs have already made headway in e-mail outsourcing and providing remote access services. The ISP configuration of i-Planet software gives ISPs a high degree of leverage for centralized control, administration, and economy of scale by hosting the gateway and server systems in the ISP network itself. This approach enables ISPs to build expertise more quickly, reduce costs of on-site visits, and employ flexible use-based billing approaches.

Enterprise Configuration

The enterprise configuration requires ISPs to install both the gateway and server systems at the business customer's site. The standard approach is to locate the gateway system in the company's Demilitarized Zone (DMZ), with the server system being located in the company's internal network where the other company resources are located (Figure 3). Remote users can then access the company from anywhere on the Internet, including telecommuter PCs and workstations, airport and hotel kiosks, and systems that are behind other firewalls — including branch and remote offices, customer sites, and supplier locations.

Gateway Configuration

The gateway is located in the DMZ along with other servers that would typically exist in a large company's network — for example an external Web server, mail gateway, and Web proxy / cache server. The core router and firewall combination allows only SSL traffic to the i-Planet technology gateway. The gateway, in turn, passes all allowable traffic on to the internal network. The gateway frequently contacts the i-Planet server system, as it provides authentication services, the home page, and access to built-in applications.

Because access from the gateway to internal servers is allowed, the security implications must be carefully considered. The fortified i-Planet technology gateway results in a system that is highly-resistant to attack. For example, even if address spoofing in the DMZ is successful, responses from the internal network will still be routed to the gateway system, not to an intruder.

Figure 3 depicts three options for configuring the gateway system:

- The first option, and the one recommended by Sun, is to place the gateway system in the DMZ, allowing incoming packets on the SSL port to reach the system, and allowing traffic from the gateway to internal services to pass through the firewall. The use of a firewall to filter traffic adds a level of security, and enables all packets bound for the internal network to be logged. In addition, the use of network switches — rather than hubs — prevents snooping from any other system in the DMZ.

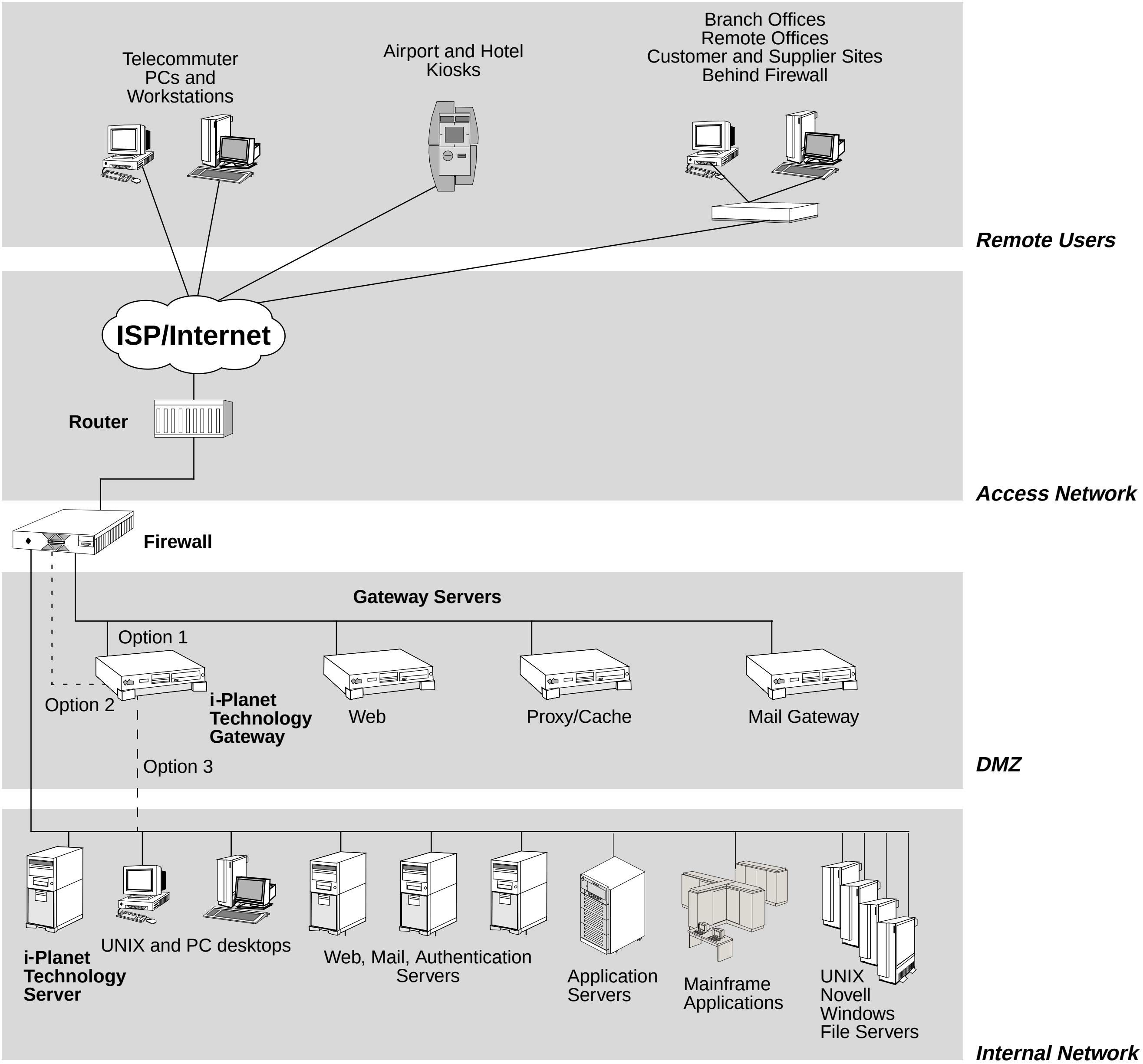

Figure 3 Enterprise configuration of i-Planet software illustrating the gateway located in the DMZ and the server in the organization's internal network.

- The second option, illustrated with a dotted line, is to pass traffic from a second network interface on the gateway system to a separate network connection on the firewall. This isolates traffic bound for the internal network, but also requires configuring an additional network interface on the firewall.
- The third option, illustrated with a dashed line, is to use a second network interface that directly connects to the internal network. Although this approach would have the lowest latency of the three options, traffic is more difficult to log, because it is not routed through a central choke point.

In all three scenarios, every packet entering the gateway is proxied and decrypted. The gateway never acts as a router, so no traffic can pass through this system un-inspected.

Server Configuration

Most of the value-added customization that an ISP could perform for business customers is on the server. This is where the Web server that hosts the home page resides, where interfaces to existing authentication services must be configured, and where user profiles are stored. In addition, access to internal file servers and desktop systems is configured on the server. Because each customer's requirements and security concerns are different, ISPs can lend their experience with i-Planet software to custom configure the servers.

ISP Configuration

The ISP configuration model involves centralized installation and administration of the i-Planet technology gateway and server platforms. This model assumes that the ISP hosting i-Planet software for business customers is the same ISP that provides them with their basic Internet connectivity. This is the most common relationship, since most small- and medium-sized businesses acquire their Internet services from ISPs.

To implement this outsourcing model, ISPs configure i-Planet technology servers in pairs (Figure 4). This gives each customer a dedicated gateway and server, with access through a URL within the customer's own domain. The ISP extends the private network between the gateway and server into the business customer's private network. The effect of this approach is that the server — though hosted at the ISP site — appears as part of the business customer's internal network, and provides authorized remote users with internal access.

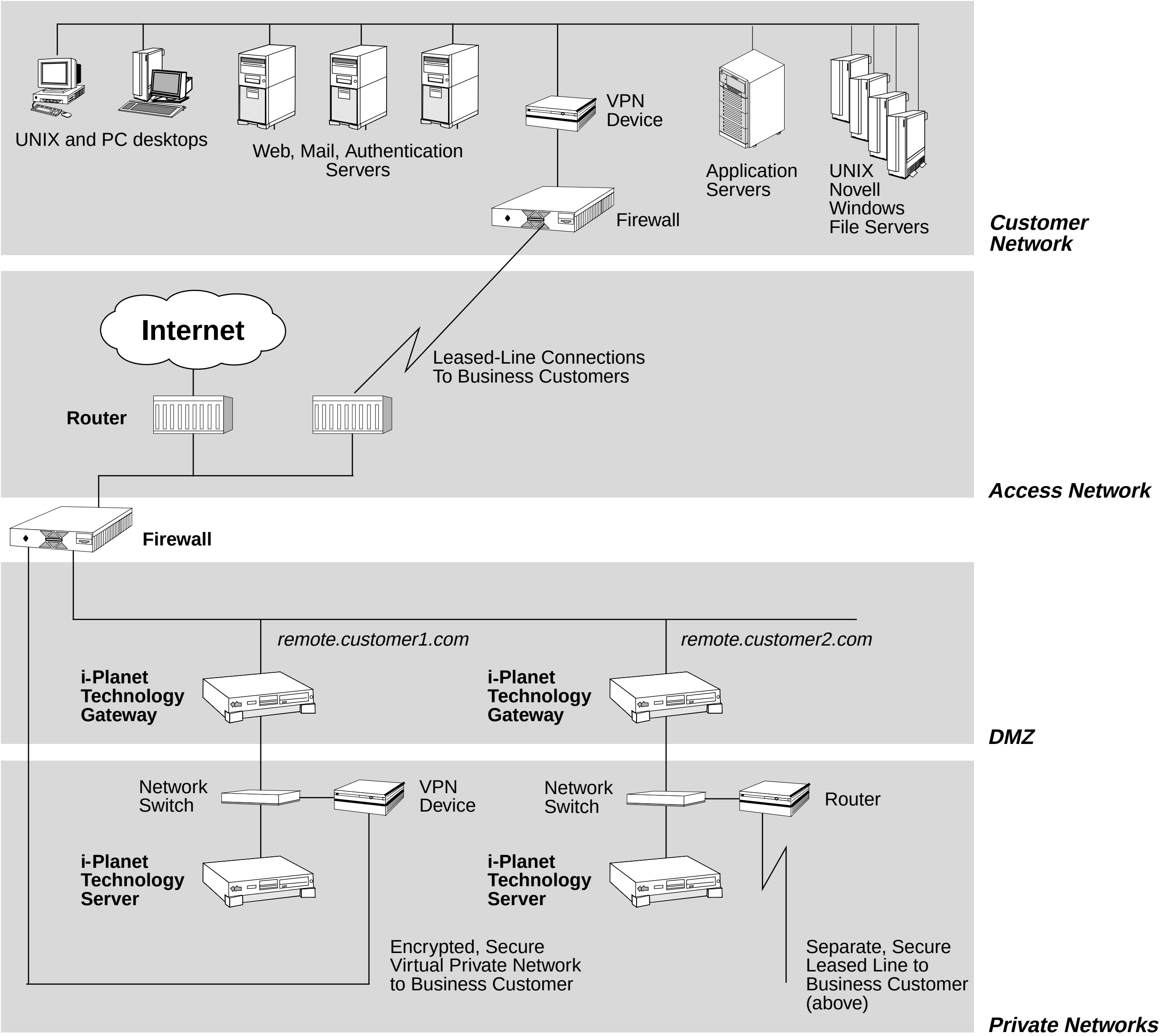
UNIX and PC desktops
Web, Mail, Authentication Servers
VPN Device
Application Servers
UNIX Novell Windows File Servers
Firewall
Customer Network
Internet
Leased-Line Connections To Business Customers
Router
Access Network
Firewall
remote.customer1.com
remote.customer2.com
i-Planet Technology Gateway
i-Planet Technology Gateway
DMZ
Network Switch
VPN Device
Network Switch
Router
i-Planet Technology Server
i-Planet Technology Server
Encrypted, Secure Virtual Private Network to Business Customer
Separate, Secure Leased Line to Business Customer (above)
Private Networks

Figure 4 ISP configuration showing two business customers supported at the ISP site; private traffic to the first customer (left) is routed through a virtual private network into the company's network; private traffic to the second customer (right) is routed via leased line to the company's network.

Two approaches that extend the small private network at the ISP site to the customer's internal network are illustrated:

- *Using Virtual Private Networks*

  The first approach (left side of Figure 4) is to configure a VPN router on the private network that routes encrypted traffic through the ISP's firewall, into a core router, and over a leased-line to the customer site. The encrypted traffic is passed through the customer's firewall and to a VPN router on the customer's internal network, where it is decrypted.

- *Using Dedicated Leased Lines*

  The second approach (right side of Figure 4) uses a standard network router to move private traffic over a dedicated leased line to the customer site. This approach is clearly more costly in terms of monthly charges, however the use of a dedicated leased line guarantees bandwidth for remote access users.

Technical Considerations

Sun has designed the i-Planet product to address security, performance, scalability, reliability, and ease of administration requirements. These qualities are further enhanced when i-Planet software is deployed following Sun's recommendations.

Security

The entire i-Planet product architecture was designed from the ground up to provide secure remote access to users on the Internet. For example, the gateway system proxies absolutely every packet from the Internet that is destined for servers on the internal network. Fortified with SunScreen dynamic packet-filtering technology, the gateway system is impervious to everything but denial-of-service attacks to which any Internet server is susceptible.

The DMZ in the ISP configuration is populated with a homogeneous set of gateway systems, and it is virtually impossible to penetrate one gateway from another system in the DMZ. This is because each gateway is as secure as the other — tightly 'locked down' with all ports closed but SSL.

The dedicated hosting model — with each customer allocated a private pair of servers — adds to the security of the i-Planet technology outsourcing model. By eliminating all chance of software-level interaction between different business customers' private data, each server is as secure as it would be if located on customer premises.

Performance

Although the gateway and server software can be configured to run on the same physical system, Sun recommends the use of two servers because of the need to simultaneously handle computationally-intensive workloads on both the gateway and server. During periods of peak activity, the gateway must perform computationally-intensive encryption and decryption with minimal impact on network latency. And while the gateway is occupied with security activities, file access involves the server in computationally-intensive file compression activities that use server horsepower to minimize the Internet bandwidth required for transferring files.

Due to the level of computation required, Sun recommends the use of a 300 MHz or faster UltraSPARC processor in each system. The Sun Enterprise Ultra 5S server meets these requirements, which is why it is the server featured in the network diagrams in this chapter. The Sun Ultra 5S server comes with a 333 MHz UltraSPARC-IIi processor accelerated with a 2 MB cache, and 512 MB of main memory. It comes standard with 9.1 GB IDE drive, 32x CD-ROM drive, floppy, 10/100 Mbps Ethernet, and three PCI bus expansion slots. For the ISP configuration illustrated in this chapter, the gateway requires a second PCI bus-based Ethernet interface.

Scalability

Enterprises of all sizes will be interested in remote access using i-Planet software, and it is likely that some applications will require more than the 333 MHz UltraSPARC processor provided in the Ultra 5S platform. Likewise, as the capabilities of remote access using i-Planet software are put to use by increasing numbers of employees in each hosted company, ISPs will need to scale the processing power of the gateway and server platforms.

Fortunately, Sun has the most scalable set of server platforms available anywhere. Beginning with the single-processor Ultra 5S server, ISPs can deploy increasing amounts of processing power using the dual-processor

Enterprise 250 server, and the quad-processor Enterprise 450 server. With up to 14 processors in the Enterprise 4500, 24 processors in the Enterprise 6500, and 64 processors in the Sun Starfire server, virtually any remote access needs can be met. Of course ISPs need servers that can deliver the power of the underlying hardware and with high reliability, which is why the Solaris Operating Environment™ is used to host Sun's i-Planet product.

In order to help ISPs plan the correct server capacity for their business customers, Sun is preparing precise guidelines that will enable ISPs to determine the processing power required by each platform to handle the different remote access workloads of their customers. When completed, these guidelines will be presented in a future version of this paper, helping readers to understand the relationship between desired throughput and the processing power required.

In the first release of i-Planet software, processing power is vertically scaled with the configuration of additional processors in a Sun Enterprise server, or with the use of increasingly larger servers. Horizontal scalability is planned for future versions, and will enable ISPs to deploy multiple systems for each function in the i-Planet software architecture, which will also increase overall service availability.

Reliability

The combination of Sun UltraSPARC processor-based servers and highly-reliable Solaris software is very reliable — with many Sun Enterprise servers and StorEdge™ storage systems providing dual, hot-swappable power supplies, disk drives, memory, I/O devices, and even processors.

The reliability of remote access through i-Planet software is only as good as the remote systems which are being accessed. Many companies have already utilized horizontally-scaled services to enhance reliability — for example, companies use multiple mail servers so that, in the event of a failure, users can continue to access their mail on the remaining systems.

Using future enhancements to Sun's Netlet technology, ISPs will be able to configure remote access clients to utilize horizontally-scaled servers in the same way as local clients. The configuration manager specifies which port the Java applet should listen to on the remote system, and which destination host and port the traffic should be directed to in the company's internal network. This information is provided in tabular form (Table 1), and will allow the specification of multiple remote hosts for the same local port — enabling a round-robin style balancing of load and progression to the next server in the event that the first server does not respond to the user request.

The configuration in Table 2 specifies two different hosts for incoming e-mail via the IMAP protocol, and two different mail gateways for outbound e-mail via the SMTP protocol.

Listen Port	Destination Host	Destination Port	Encrypt?
143 (IMAP)	mail1.company.com	143	yes
143 (IMAP)	mail2.company.com	143	yes
25 (SMTP)	gw1.company.com	25	yes
25 (SMTP)	gw2.company.com	25	yes

Table 1 Future versions of the Netlet will enable round-robin access to multiple systems, enabling the use of horizontally-scaled servers at the business customer site.

Ease of Administration

Sun’s i-Planet software is administered through simple, intuitive graphical user interfaces provided by the server and made available only to users on the internal network. This presents a potential problem for ISPs using either of the configurations discussed in this chapter. When ISPs deploy the enterprise configuration, they require remote administration capabilities, saving visits to customer sites. Likewise, in the ISP configuration, remote administration is necessary in order to service the needs of many business customers from a single administration console.

Specific remote administration features are intentionally not provided as part of the i-Planet product because the power of Netlet technology provides a graceful solution. Administrators can configure the server with a special administration page that downloads a pre-configured Netlet to the administrator’s Web browser. The configuration table re-directs local HTTP requests to port 80 to the server’s administration port (8080), as illustrated in Table 2.

Listen Port	Destination Host	Destination Port	Encrypt?
80 (HTTP)	server.company.com	8080	yes

Table 2 Netlet technology can be used to extend administration server access to authorized remote administrators.

In order to access the administration server, a remote user would first be required to provide acceptable authentication information to the i-Planet product's login page. After accessing the administration console simply through *http://localhost*, a second level of authentication would then be required for access to the administration server — all of this performed using SSL-encrypted communication to the i-Planet technology gateway.

ISP Value-Added Services

This chapter has illustrated two approaches that ISPs can use to provide value-added remote access services to business customers. It has outlined a few of the many additional configuration services that experienced ISPs can provide. These services include customized access to multiple or partitioned mail hosts, access to additional authentication mechanisms, and remote administration for ISP and customer use.

When companies adopt the i-Planet remote access model, their cost burden shifts from supporting and maintaining the dial-in/VPN paradigm to providing Internet access so that remote employees can access internal services securely over the Internet. Key to providing this access to authorized users is the concept of *roaming*. Roaming allows users to connect to an ISP's point-of-presence with a local call without requiring an account at the ISP at all — enabling worldwide access without having ISP accounts in every country. When ISPs provide i-Planet technology-based services combined with roaming capabilities, they complete the compelling package of services that can help their business customers shift from costly, dial-up remote access to secure ubiquitous access using the Internet.

Getting Started 4

The advent of i-Planet software from Sun Microsystems changes the very nature of the way organizations can provide remote access to authorized IT systems. Rather than enduring the high costs of maintaining dial-up and leased-line connections, client hardware and software, and VPN technology, companies can now enable their employees, remote offices, customers, consultants, and suppliers to access their IT systems in a secure manner. Software, support, and maintenance costs plummet because the only client software required for access through the i-Planet product is a Java technology-enabled Web browser.

The overwhelming response of executives who have seen the i-Planet product in action is the desire to have it available to their own companies. This presents a unique window of opportunity for Internet Service Providers to provide i-Planet software-based remote access services for their small- and medium-sized business customers. The enterprise configuration provides ISPs with the opportunity to use their expertise in setting up and remotely maintaining customer premises installations of the i-Planet product. The ISP configuration enables Internet Service Providers to consolidate the required hardware in their data center and use their expertise to support large numbers of customers from a central location.

The key to building a successful business model based on provisioning outsourced remote access is the ability to quickly build expertise that leaves competitors behind the learning curve. There are many ways to configure and extend the services provided by i-Planet software. ISPs that quickly build a customer base keep ISP technical staff up-to-speed at providing sophisticated services that exceed the capabilities of small- and medium-sized business customers.

The first step is to choose an initial customer for a pilot deployment of either configuration model. Rapid deployment will prove the benefits of i-Planet software, generate a reference customer, and build expertise in the ISP organization. The initial investment of two Sun Ultra 5S servers prepares ISPs to roll-out i-Planet technology-based services to other business customers.

Sun's i-Planet product provides ISPs with an easy way to offer value-added services to their customers. It is available on the platforms most preferred by ISPs today — reliable and scalable servers from Sun Microsystems. Sun's entry-level servers meet the needs of small companies to economically provide secure remote access through i-Planet software. To accommodate larger companies — and small companies with growing remote access requirements — Sun's multiprocessor Enterprise servers can scale from two to 64 processors, with binary compatibility and the reliability, availability, and serviceability features that are so critical for operation in ISP environments. For lights-out operation in telephone company ISP environments, Sun's Netra™ t servers provide single- and dual-processor capabilities in a rugged, NEBS Level-3 certified package which ensures carrier-grade reliability. With servers to support i-Planet product deployments in the smallest companies to the largest enterprises, the choice of Sun's i-Planet remote access technology will sharpen any ISP's competitive edge.

References 5

Sun Microsystems posts product information in the form of data sheets, specifications, and white papers on its Internet Web page at *http://www.sun.com/*.

HEADQUARTERS **SUN MICROSYSTEMS, INC.,** 901 SAN ANTONIO ROAD, PALO ALTO, CA 94303-4900 USA
PHONE: 650 960-1300 FAX: 650 969-9131 INTERNET: www.sun.com

THE NETWORK IS THE COMPUTER™

SALES OFFICES

AFRICA (NORTH, WEST, AND CENTRAL) +33-1-30674680 • **ARGENTINA:** +54-1-317-5600 • **AUSTRALIA:** +61-2-9844-5000 • **AUSTRIA:** +43-1-60563-0 • **BELGIUM:** +32-2-716-79-11 • **BRAZIL:** +55-11-5181-8988 • **CANADA:** +905-477-6745 • **CHILE:** +56-2-3724500 • **COLOMBIA:** +571-629-2323 • **COMMONWEALTH OF INDEPENDENT STATES:** +7-502-935-8411 • **CZECH REPUBLICS: CZECH:** +420-2-33-00-93-11 • **DENMARK:** +45-4556-5000 • **ESTONIA:** +372-6-308-900 • **FINLAND:** +358-9-525-561 • **FRANCE:** +33-01-30-67-50-00 • **GERMANY:** +49-89-46008-0 **GREECE:** +30-1-618-8111 • **HUNGARY:** +36-1-202-4415 • **ICELAND:** +354-563-3010 • **INDIA:** +91-80-5599595 • **IRELAND:** +353-1-8055-666 • **ISRAEL:** +972-9-9513465 • **ITALY:** +39-039-60551 • **JAPAN:** +81-3-5717-5000 • **KAZAKHSTAN:** +7-3272-466774 **KOREA:** +822-3469-0114 • **LATVIA:** +371-755-11-33 • **LITHUANIA:** +370-729-8468 • **LUXEMBOURG:** +352-49-11-33-1 • **MALAYSIA:** +603-264-9988 • **MEXICO:** +52-5-258-6100 • **NETHERLANDS:** +31-33-450-1234 • **NEW ZEALAND:** +64-4-499-2344 **NORWAY:** +47-2202-3900 • **PEOPLE'S REPUBLIC OF CHINA: BEIJING:** +86-10-6803-5588; **CHENGDU:** +86-28-619-9333; **GUANGZHOU:** +86-20-8777-9913; **HONG KONG:** +852-2802-4188; **SHANGHAI:** +86-21-6466-1228 • **POLAND:** +48-22-8747800 **PORTUGAL:** +351-1-412-7710 • **RUSSIA:** +7-502-935-8411 • **SINGAPORE:** +65-438-1888 • **SLOVAK REPUBLIC:** +421-7-522-94-85 • **SOUTH AFRICA:** +2711-805-4305 • **SPAIN:** +34-1-596-9900 • **SWEDEN:** +46-8-623-90-00 • **SWITZERLAND:** +41-1-825-7111 • **TAIWAN:** +886-2-2514-0567 **THAILAND:** +662-636-1555 • **TURKEY:** +90-212-236-3300 • **UNITED ARAB EMIRATES:** +971-4-366-333 • **UNITED KINGDOM:** +44-1-276-20444 • **UNITED STATES:** +1-800-555-9SUN • **VENEZUELA:** +58-2-905-3800 • **WORLDWIDE HEADQUARTERS:** +1-650-960-1300

LFC9.0 Printed in USA 4/99 FE971-0/2.5K