PeopleSoft Red Paper Series

Securing Your PeopleSoft Application Environment

July 2010

Including:

- How to Plan for Security
- How to Secure Customized System
- Exposing PeopleSoft outside the Firewall

ORACLE

PEOPLESOFT ENTERPRISE

Securing Your PeopleSoft Application Environment

Restricted Rights

Comments on this document can be submitted to peopletools_ww@oracle.com. We encourage you provide feedback on this Red Paper and will ensure that it is updated based on feedback received. When you send information to Oracle PeopleSoft, you grant Oracle PeopleSoft a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Extensive reference is made to PeopleBooks -
http://www.oracle.com/pls/psft/homepage

This document is subject to change without notice, and Oracle PeopleSoft does not warrant that the material contained in this document is error-free. If you find any problems with this document, please report them to Oracle PeopleSoft in writing.

This material has not been submitted to any formal Oracle PeopleSoft test and is published AS IS. It has not been the subject of rigorous review. Oracle PeopleSoft assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by Oracle PeopleSoft for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk
Information in this book was developed in conjunction with use of the product specified, and is limited in application to those specific hardware and software products and levels.

Oracle PeopleSoft may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

.

TABLE OF CONTENTS

Chapter 1 - Introduction

This red paper is a practical guide for technical users, installers, system administrators, and programmers who implement, maintain, or develop applications for your PeopleSoft system. This red paper discusses guidelines on how to address the security of your implementation, including network infrastructure considerations, hardening of the PeopleSoft Internet Architecture and Portal, and other system-hardening configuration recommendations. This document doesn't cover the configuration of batch processes.

The information contained in this document originated from many sources, including industry research and knowledge, internal expertise, and Oracle Global Customer Support (GCS), and therefore contains "real-life" solutions and recommendations that have been implemented in the field. Because we can't address every security consideration that might be applicable to your specific implementation and environment, the items discussed in this document are intended to give a broad "recommended guidelines" baseline for securing an Oracle PeopleSoft environment. As such, many of the frequently asked questions we receive from the field are covered in this document.

STRUCTURE OF THIS RED PAPER

This red paper provides guidance in setting up security for Oracle PeopleSoft systems beyond application security. The intent of this document is to provide information about securing the overall infrastructure of a deployed PeopleSoft system.

- Chapter 1, "Introduction," introduces the red paper.
- Chapter 2, "Security Model," discusses required reading and gives a conceptual overview of security issues. Individuals and groups who may be tasked with setting security policy as well as ensuring compliance and adherence to industry best practices should find this section useful.
- Chapter 3, "Securing Network Infrastructure," discusses different approaches to network infrastructure security. Network and security administrators (or other individuals tasked with network security) will find useful guidelines in this section for securing the supporting network of a PeopleSoft environment.
- Chapter 4, "Securing PeopleSoft Internet Architecture," gives practical solutions for Pure Internet Architecture (PIA) security. It is a practical guide to providing security solutions and recommended settings for providing and maintaining PIA security. System and Security Administrators should find this information useful.
- Chapter 5, "PeopleTools Security Hardening," discusses hardening of PeopleTools Security. System administrators should find valuable information in this section about how to address hardening and improving PeopleTools Security
- Chapter 6, "Securing Customized PeopleSoft Applications," gives some guidelines securing a customized application. Developers, system administrators, and business analysts can find guidance and recommendations for good security practices when customizing applications in this section.

Note that Oracle PeopleSoft updates this document as needed so that it reflects the most current feedback we receive from the field. Therefore, the structure, headings, content, and length of this document are likely to vary with each posted version. To determine whether the document has been updated since you last downloaded it, compare the date of your version to the date of the version posted on Customer Connection.

RELATED MATERIALS

This paper is not a general introduction to environment tuning, and we assume that our readers are experienced IT professionals, with a good understanding of the PeopleSoft internet architecture. To take full advantage of the information covered in this document, we recommend that you have a basic understanding of system administration, internet architecture, relational database concepts, SQL, and how to use PeopleSoft applications.

This document is not intended to replace the documentation delivered with the PeopleTools electronic delivery, media packs, or PeopleBooks (note that you should reference those documents appropriate to your specific version of PeopleSoft products). We recommend that before you read this document, you read the PIA-related information in the PeopleTools PeopleBooks to ensure that you have a well-rounded understanding of PIA technology.

Note. Much of the information in this document will eventually be incorporated into subsequent versions of the PeopleBooks.

Many of the fundamental concepts related to PIA are discussed in the following documents:

Enterprise PeopleTools PeopleBooks

- System and Server Administration
- Security Administration
- PeopleSoft Application Designer
- PeopleSoft Integration Broker
- PeopleCode Language Reference

Separate PeopleSoft documents:

- PeopleSoft Installation and Administration
- PeopleSoft Hardware and Software Requirements

Additionally, we recommend that you read the Tuxedo and Weblogic documentation on oracle.com.

Chapter 2 - Security Model

REQUIRED READING

A number of books, publications, and white papers on security are available that a security administrator should consult to get a comprehensive understanding of how to secure a site. At a minimum, please download and read *Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices*, published by Internet Security Alliance, from http://www.isalliance.org/iRequestForm.

The document is an excellent starting guide for security administrators to ensure that basic security policies and practices are observed within an organization before any PeopleSoft-specific security is put into place. The document identifies ten of the highest-priority and most-frequently recommended security practices as a place to start for today's operational systems. These practices address dimensions of information security such as policy, process, people, and technology, all of which are necessary for deployment of a successful security process. Each organization is responsible for determining where to position itself on this exponential curve (a symbolic reference to the full spectrum of "dimensions of information security") and what amount of security investment they need to make to achieve a satisfactory level of security within the system. A satisfactory level of security also depends on the business goals of the security system. These considerations lead us to the need to create a security model targeted to address security threats and their business impact.

SECURITY MODEL – A CONCEPT

When it comes to information security, there are no silver bullets—no one process, technology, or certification that will guarantee 100% safety. Industry best practices dictate that an organization use a combination of processes and technologies that mitigate risk and limit damage. Security comprises three main areas: planning, prevention, and response. Without a plan, your company will not be well-prepared to repel attacks and deal with intrusions. Techniques and tools targeted at prevention should be where most of your energy and funding are directed. In the event that prevention fails, you must be ready to respond quickly and masterfully.

Keeping this in mind, the first step in securing a PeopleSoft environment is to create a security model for your site at the enterprise or organizational level. You can create a new model, or align your PeopleSoft security implementation strategy with your existing security model. One of the biggest errors that an organization can make when deploying new services, systems, and technologies is failing to align security capabilities with business objectives. Your organization should develop or leverage a security model that manages the inherent trade-offs between enablement and protection of an enterprise's most valuable resource—its information assets.

Let us first explain what we mean by *security model*. A security model is a formal description of a security policy. This naturally leads to the question: What is a security policy?

- A security policy should capture the security requirements of an enterprise, or describe the steps that must be taken to achieve security.
- Security models are used in security evaluation, and sometimes for proof of security.

Current wisdom has identified three widely accepted legs of security:

- Computer Security – Use risk assesment, apply the CIA+ taxonimy (Confidentiality, Integrity, Avialability, non-repudiation, and authentication), new goals and extended enterprise planning models.
- Physical Security – Integrate physical access systems with network authorization systems.
- Trustworthy People – Know whom you give access to. Apply due diligence.

Many security models are available that an organization can apply in an effort to meet the security criteria specific to that organization that are based upon their business processes and requirements as well as the level of risk they have determined to be acceptable (this can be driven by many criteria, ranging from customer demands to industy-standard practices to regulatory requirements).

The following discussion highlights a few of the more common security models.

The classic (traditional) security model followed by many organizations is what has come to be known as the CIA Model. This model focuses on the *Confidentiality*, *Integrity*, and *Availability* aspects of security. Many in the security industry would state that these core tenets are the ultimate goal of information security. However, other considerations exist that this approach may not address. Forged in the early days of the internet's commercialization, the classic CIA approach also took on *authentication*, *access control*, and *nonrepudiation* as goals in the mid-1990s. Since then, this model has become standard security fare. But this goal-oriented approach neglects today's critical security needs, where attacks are more sophisticated and frequent and come from a wider range of sources. For example, the traditional architecture for implementing the CIA model—the firewall-based perimeter—is increasingly ineffective. Worse still, the goal-oriented approach doesn't address the other half of good security planning: risk assessment. Risk assessment, which guides security managers in prioritizing security spending, is sorely neglected even in organizations that acknowledge its importance.

The CIA model is a good foundation to achieve high security. However, while it does a great job of addressing confidentiality and its five siblings as tried-and-true security goals, it is critical to understand that these goals are only part of the plan. Other goals should be risk assessment and the creation of a modified version of a *demilitarized zone* (DMZ) perimeter. Critical, too, is the need to recognize new goals as they emerge.

Several other security models are also available:

- Many security consulting organizations have devised an alternative security model that identifies security more as a ***"strategic business process that includes the organisation, the processes, and the technologies that enable access to, and protection of, an enterprise's information assets."*** This comprehensive security model illustrates how to identify, create, capture, and sustain the value of security in an organization by managing the inherent trade-offs between enablement and protection of an enterprise's most valuable resource—its information assets. In this model, these primary security activities are driven by business objectives and carried out in alignment with the enterprise's supporting capabilities—its organization (people), robust processes, and technology infrastructure. This type of model centers on how security adds value to an organization. A security model of this nature is specifically designed to function as a road map. It helps an organization navigate the process of building a scalable and sustainable security infrastructure that both protects and enables access to critical business and information assets in alignment with strategic business objectives and appropriately balanced and associated costs.
- Another alternative has been developed by the Burton Group; it is commonly referred to as the *Virtual Extended Network* (VEN) model. The goal-oriented CIA model discussed previously often results in what many industry analysts call a "tootsie pop" syndrome—that is, a security model that results in a hard shell with a soft chewy center infrastructure. The CIA model can produce significant security weakness, especially in light of the pervasiveness of web-enabled applications and systems. Allowing users to do anything possible once they're inside is no longer sufficient.

  The VEN model is an alternative to the traditional DMZ. It consists of four layers that represent different techniques for different zones of use:

  - Resource – network, servers, data.
  - Control – employees and security systems.
  - Perimeter – partners.
  - Extended Perimeter – suppliers and customers.

  Specifically, the VEN model defines four logical layers: the resource layer, which houses clients, servers, applications and data; the control layer, where authentication services reside, as do controls for security policies across layers; the perimeter layer, which defines an organization's physical boundaries and contains firewalls, proxies, and gateways; and the extended perimeter, where companies engage technologies or services to secure resources that are physically located outside the perimeter. The result is a model that builds on the existing infrastructure, but plans for a distributed perimeter.

Security is an integration of people, processes, and technology. Rather than being merely a technology fix, security must now be defined in a way that incorporates the critical roles and interdependence that exist between an organization's people, its firm processes, and its technology infrastructure. Leveraging a clearly defined security model will enable your organization to address these issues in combination, resulting in a PeopleSoft environment that provides a world-class security posture.

The security model is essential to create critical requirements that support a secure enterprise. The success of these initiatives, however, hinges on several critical requirements, with profound implications for any organization:

- Technology resources are connected and available to the appropriate users.

- Checks and balances exist to ensure appropriate access and approvals.
- Perimeter protection and monitoring are assured.
- The supporting infrastructure:
  - Is resilient under variable circumstances.
  - Is reliable under all conditions.
  - Performs.
  - Scales.
  - Supports interoperability.
  - Is efficiently maintained.

This document does not provide a lengthy discussion about security models and how to develop and implement them, but it is critical to understand that the securing of your PeopleSoft environment should be done in alignment with your enterprise security policies. Those policies should be created from the foundation based upon the security model that you've established. Securing your PeopleSoft environment should not be a one-off solution, but rather a comprehensive approach taken in concert with overall corporate security policies, guidelines, and business requirements.

SECURITY THREATS

In order to secure a site or organization, the first thing to know is where the security threats exist, how these threats are exploited, and what the financial ramifications are for each of these threats. The primary step in addressing security threats is to conduct and periodically repeat an information security risk evaluation that identifies your critical information assets (for example, systems, networks, and data), threats to critical assets, asset vulnerabilities, and risks.

A security assessment should include the following tasks:

- Identify the adverse impacts when risks to critical assets are exploited, including financial, reputation, market position, time and productivity, and so on.
- Quantify the financial impact to the greatest extent possible.
- Develop and implement a risk mitigation plan resulting from the evaluation, and keep it updated.
- Ensure that there are regular review and management of the risks to critical information assets.

A critical part of addressing security threats is to identify and properly secure the systems deployed within your infrastructure and organization. This security assessment enables you to create a list of security vulnerabilities for the deployed software and hardware. An additional resource for identifying known vendor-specific vulnerabilities and the associated patches or remediation is available at http://www.securityfocus.com/bid/.

Create a list of all vendors, including PeopleSoft, who have supplied software and hardware for the deployed system. Then for each vendor and their hardware, software, or both, create a list of known vulnerabilities. This list provides a list of known issues and security concerns, and at a minimum these should be addressed. This might include applying patches, identifying workarounds, and implementing them during deployment.

The list of known vulnerabilities and the results of the security assessment will provide your organization with a remediation road map for improving the security posture of your PeopleSoft environment. It is crucial to actually implement the fixes, patches, and recommended security infrastructure improvements. In many cases, significant improvements in overall security can be achieved with minimal levels of effort (man-hours) or costs. In short, action *is* a requirement. Failure to implement remediations or address discovered vulnerabilities and risks will leave your entire infrastructure at risk.

SECURITY: A DEFENSE-IN-DEPTH APPROACH

Defense-in-depth is a practical strategy for achieving information security (often called *information assurance*) in today's highly networked environments. It is a best practices strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability and cost, performance, and

operational considerations. It is also important to resist detrimental effects from nonmalicious events such as fire, flood, power outages, and user error.

The defense-in-depth approach builds mutually supporting layers of defense to reduce vulnerabilities and to assist an organization in its efforts to protect against, detect, and react to as many attacks as possible. The construction of mutually supporting layers of defense inhibits the ability of an adversary who penetrates or breaks down one defensive layer to promptly encounter another, and another, until the attack is ultimately thwarted. To protect against different attack methods, it is important to employ corresponding security measures. The weakness of one security measure should be compensated for by the strength of another.

To effectively resist attacks against its information and information systems, an organization needs to characterize its adversaries, their potential motivations, and their classes of attack. Potential adversaries might include nation states, terrorists, criminal elements, hackers, or corporate competitors. Their motivations might include intelligence gathering, theft of intellectual property, denial of service, embarrassment, or just pride in exploiting a notable target. Their classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation of insiders, and attacks through the industry providers of information technology resources.

The goal of implementing a security model is to provide information security and protection (assurance). This goal is realized when information and information systems are protected against such attacks through the application of security services discussed previously in the chapter, such as availability, integrity, authentication, confidentiality, and nonrepudiation. The application of these services should be based on the *Protect, Detect, and React* paradigm. This means that in addition to incorporating protection mechanisms, organizations should expect attacks and employ attack detection tools and procedures that enable them to react to and recover from these attacks.

An important principle of the defense-in-depth strategy is that achieving information assurance requires a balanced focus on three primary elements: people, technology, and operations. These areas of attention correlate very well with the three primary elements of the defense-in-depth approach to security:

- **People.** Achieving information assurance begins with a commitment by senior management (typically at the chief information officer level) based on a clear understanding of the perceived threat. This must be followed through with effective information assurance policies and procedures, assignment of roles and responsibilities, commitment of resources, training of critical personnel (for example, users and system administrators), and personal accountability. This includes the establishment of physical security and personnel security measures to control and monitor access to facilities and critical elements of the information technology environment.
- **Technology.** Today, a wide range of technologies is available for providing information assurance services and for detecting intrusions. To ensure that the right technologies are procured and deployed, an organization should establish effective policies and processes for technology acquisition. These should include a security policy, information assurance principles, system-level information assurance architectures and standards, criteria for needed information assurance products, acquisition of products that have been validated by a reputable third party, configuration guidance, and processes for assessing the risk of the integrated systems.
- **Operations.** The operations element focuses on all the activities required to sustain an organization's security posture on a day-to-day basis. These include:
  - Maintaining visible and up-to-date system-security policy.
  - Certifying and accrediting changes to the information technology baseline.
  - Managing the security posture of the information assurance technology.
  - Providing key management services and protecting the infrastructure.
  - Performing system security assessments.
  - Monitoring and reacting to current threats.
  - Incident response.
  - Disaster recovery and business continuity.

Defense-in-Depth Summary

The key aspects of defense-in-depth are that it's layered, comprehensive, tested and proven, flexible rather than brittle, and requires knowledge and skill. While anticipating every contingency isn't possible, developing a well-rounded information security plan can help to dissuade all but the most determined attackers. With proper auditing systems such as audit logs, intrusion detection systems, and other mechanisms, incident response staff will have the right tools to determine what happened should a successful attack occur. Finally, note that maintaining confidentiality, integrity, and availability of information requires significant resources, time, and money. Security is not something that can be dropped in place and forgotten.

Considering a defense-in-depth approach, securing your PeopleSoft environment requires you to implement a combination of security mechanisms and controls. These security mechanisms and controls will touch on many facets of the PeopleSoft environment. Be sure to address the following areas:

- Organization Security:
  - Security strategy.
  - Organizational awareness.
  - Internal threat profiling.
- Operations Security:
  - Security policy.
  - Recurring assessments.
- Infrastructure Security:
  - Network architecture, design, and implementation.
  - Network vulnerability assessment.
  - Operating systems, storage, and wireless security.
  - Penetration testing.
- Application Security:
  - Application architecture, design, and implementation.
  - Application penetration testing.
  - Secure software methodologies for internally developed software or modification to commercial off-the-shelf (COTS) applications.
  - Product assessments.

Chapter 3 - Securing Network Infrastructure

This chapter discusses various network components used for secure systems. Instead of covering all possible configurations and devices, this chapter addresses systems that apply to PeopleSoft architecture and that have been tested in the field. The discussion is also limited to security configuration only; scalability and high-availability configurations are discussed in the *Clustering and High Availability of PeopleSoft 8.4* red paper located on Customer Connection. The various security components to consider in your system are:

Routers – Most routers also have certain firewall capability, such as packet filtering, port blocking, and so on. These features should be enabled for added security whenever possible.

Customers using co-location will generally not have access to the router because this is part of the co-location provider's equipment. In these cases, all security features must be implemented within the system using additional equipment including firewalls, load balancer network address translation (NAT), reverse proxy server, and so on.

Firewalls – The firewall is one of the most common network devices used to secure a network environment. A firewall can be a logical or a physical device. The logical version of a firewall can be a combination of routers, load balancers, and switches working together to create a secure network. A physical firewall device can be special software running on commodity hardware, or it can be a dedicated hardware device.

In the following sections, we use a three-pronged firewall. In this configuration, the firewall has three interfaces: one for internet, one for intranet, and one for the demilitarized zone (DMZ) services. This configuration has a single point-of-protection (security failure) limitation for the intranet site. If this is not acceptable, the three-pronged firewall should be preceded with another pair of redundant firewalls. It is possible to run load balancers to distribute load among identical firewall units (FWLBS) for greater scalability, but the configuration is not simple. Implementing the three-pronged firewall with redundancy will require six extra load balancers and six extra switches/VLANS to implement.

Load Balancers – A load balancers is a highly recommended device for achieving high scalability and fault tolerance at a reasonable cost. Most units can be configured to replace a firewall and provide hardware SSL acceleration. This provides some amount of security and scalability at a reasonable cost. On most load balancers, each physical unit can be configured into multiple logical units. These logical units may have separate network interfaces and can be placed in various network topologies. Security administrators will most often not allow a single physical device to be configured for more than one security zone.

Reverse Proxy Servers – Reverse Proxy Servers (RPSs) are most often used as part of a security infrastructure. Most sites deploy them to prevent internet IP packets from reaching production web servers directly. This is a security device for inbound HTTP(S) PIA traffic. An RPS provides protection from attacks that are launched to take advantage of vulnerability such as buffer overflow, malformed packets, and so on. It also adds another tier to the security architecture. Other sites may use them as a single sign-on portal server; one that allows RPS-authenticated users to access multiple internal systems with varying authentication schemes without individual authentication to those systems.

Multiple RPSs are required for redundancy and in some cases for scalability. When multiple RPSs are deployed, a load balancer must be used in front of the RPS cluster. For PeopleSoft applications, a site domain name mapping will map to the load balancer for the RPS. For instance, an example site, *portal.corp.com*, should be mapped to a Virtual IP (VIP) 123.123.123.100 by external DNS systems and this VIP should be mapped to the RPS load balancer.

Forward Proxy Servers – Forward proxy servers, or proxy servers, are mostly used as part of a client security and caching infrastructure. Most sites deploy them to prevent users from connecting to the internet directly. This is a security device for outbound HTTP(S) PIA traffic. The user's browser connects to a proxy server that is either configured in the browser or transparently routed to via a router. The proxy does the actual communication with the web server on behalf of the user. The proxy also can cache content to improve performance and to log all browsing history for audit purposes.

In the case in which a site deploys either a PeopleSoft Integration System or an Enterprise Portal System that communicates with servers outside the production environment, a (forward) proxy server should be used. The production firewall should be configured to allow only the proxy server to connect outside the firewall. The proxy is therefore the only means of communicating with the outside world from within the production environment. All HTTP(S) requests originating from PeopleSoft servers should be routed via the proxy server.

Servers – Servers have a number of security settings and vulnerability issues associated with them. At a minimum, all vendor-provided OS security patches should be applied to the servers. Additionally, all unused services should be disabled on the servers. This is explained in detail later in this red paper.

Web servers and application servers should also use dual network interfaces so that they can reside in separate subnets. This provides additional level security layers. The merits of having a different subnet for each layer can create complicated router

policies that are required for administering servers in different subnets. Additionally, certain security failures on the web server might expose sensitive data even if the security of the application server and the database server has not been compromised.

DNS Servers – A PeopleSoft production system should avoid using DNS name resolution whenever possible. Instead, it should use statically configured server addresses. It may be necessary, however, for PeopleSoft Portal or Application Messaging to be able to access remote servers. In this case, an /etc/hosts entry is not practical and some DNS lookup may be necessary. Under no circumstances should the local DNS servers be allowed to receive DNS updates from remote servers. The local DNS server should also be prevented from sending DNS queries to a remote server for local addresses. The local DNS server should only query the remote server for addresses that are outside the local domain of the site.

Disaster Recovery Plans – All installations regardless of size must create a disaster recovery plan. The disaster recovery plan must include unavailability due to security failures, standard power failures, physical disasters, and other outages. For highly secure installations, this should include creation of a second data center that is also part of a separate physical security zone. This means separate network security policies, access codes or badges, and security administrators.

Virtual IPs (VIPs) – VIPs are not physical devices. These are IP addresses where users point their browsers to access a service. These IP addresses could point to a real web server in the simplest case. In most of the systems described in this document, they will point to a logical service implemented using firewalls, load balancers, proxy servers, and real servers. A VIP is also the IP address that the site's DNS name maps to. For instance, an example site, *portal.corp.com*, is mapped to a VIP 123.123.123.100 by external DNS systems.

Private Non-routable Address (RFC 1918) – Private non-routable addresses are IP addresses in the range 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, and 192.168.0.0–192.168.255.255. These IP addresses work within a network and all addresses within the network are addressable internal hosts and routers. These addresses are not addressable from the internet, and internet routers will not be able to route packets to these IP addresses. Having a private IP address provides some security by isolating the internal servers from the outside world, but does not preclude the need for a firewall.

Public Address – Almost all IP addresses that are not within the range mentioned in RFC 1918 are publicly addressable. These are IP addresses that can be addressed and routed over the internet. Public addresses are required to expose services to internet user.

Network Address Translation (NAT) – NAT enables a local-area network (LAN) to use Private Non-routable IP addresses for internal traffic and public addresses for external traffic. A NAT device located where the LAN meets the internet makes all necessary IP address translations to packets moving from one address space to another. NAT provides some level of security by providing stateful inspection and by isolating the internal servers from the outside world. PIA uses HTTP(S) only and has no problems with NAT. Some network software, such as IPSec, Kerberos, and so on require end-to-end packet-level integrity and will not work with NAT. In some of these cases, for example, for IPSec, performing NAT for security alone is not needed. Also, the use of NAT does not preclude the need for a firewall.

SECURE SETUPS

This section discusses some common PeopleSoft system layouts. The system layouts will have varying degrees of scalability, availability, and security. Because every site is unique with unique requirements, different parts of the layout will require modification. PeopleSoft consulting can provide that support on a case-by-case basis. The following items are basic design assumptions and policies that should be addressed.

Security

- The system should not have any single point of security failure in the architecture.
- Some security restrictions will reduce the overall scalability of the system.
- Name resolution is done using host files instead of using DNS (in most cases).
- Static routes are used within the system whenever possible.
- The PeopleSoft system has been placed on the DMZ network.
- At least one level of NAT is available from outside the network to the web server tier.
- The architecture assumes the external/internet as well as internal/intranet network to be untrusted, so protection from both the internet and the intranet is needed.
- The architecture provides at least one extra level of security layer between the DMZ and the internal network. Should the security of the DMZ become compromised, the internal network will still be protected.

- Each tier in the PeopleSoft Pure Internet Architecture has been leveraged to provide an additional security tier between the outside network and the protected data.
- Portal/Application Messaging calls from inside to outside are via a forward proxy.
- Default policy of firewall and router is to deny all.
- A three-pronged DMZ architecture is used. This has a single point of security failure limitation for the intranet site.
- Security is restricted to a single site in this version of the document. Disaster recovery over two physical security zones is not discussed in this red paper.

Scalability

- The system should be able to scale with demand as much as possible without requiring change of architecture.
- The system should scale with commodity hardware whenever possible.
- The system should scale with the most cost-effective solution.

Availability

- The system should be expandable so that no single point of failure exists in the architecture even though the configuration shown is not the expanded version.

Note that in some diagrams that follow, a redundant version of the architecture is shown although the redundancy settings of the architecture are not discussed in this document. The redundancy portion of the architecture is discussed in the *Clustering and High Availability* red paper available on PeopleSoft Customer Connection.

NAT DMZ Infrastructure

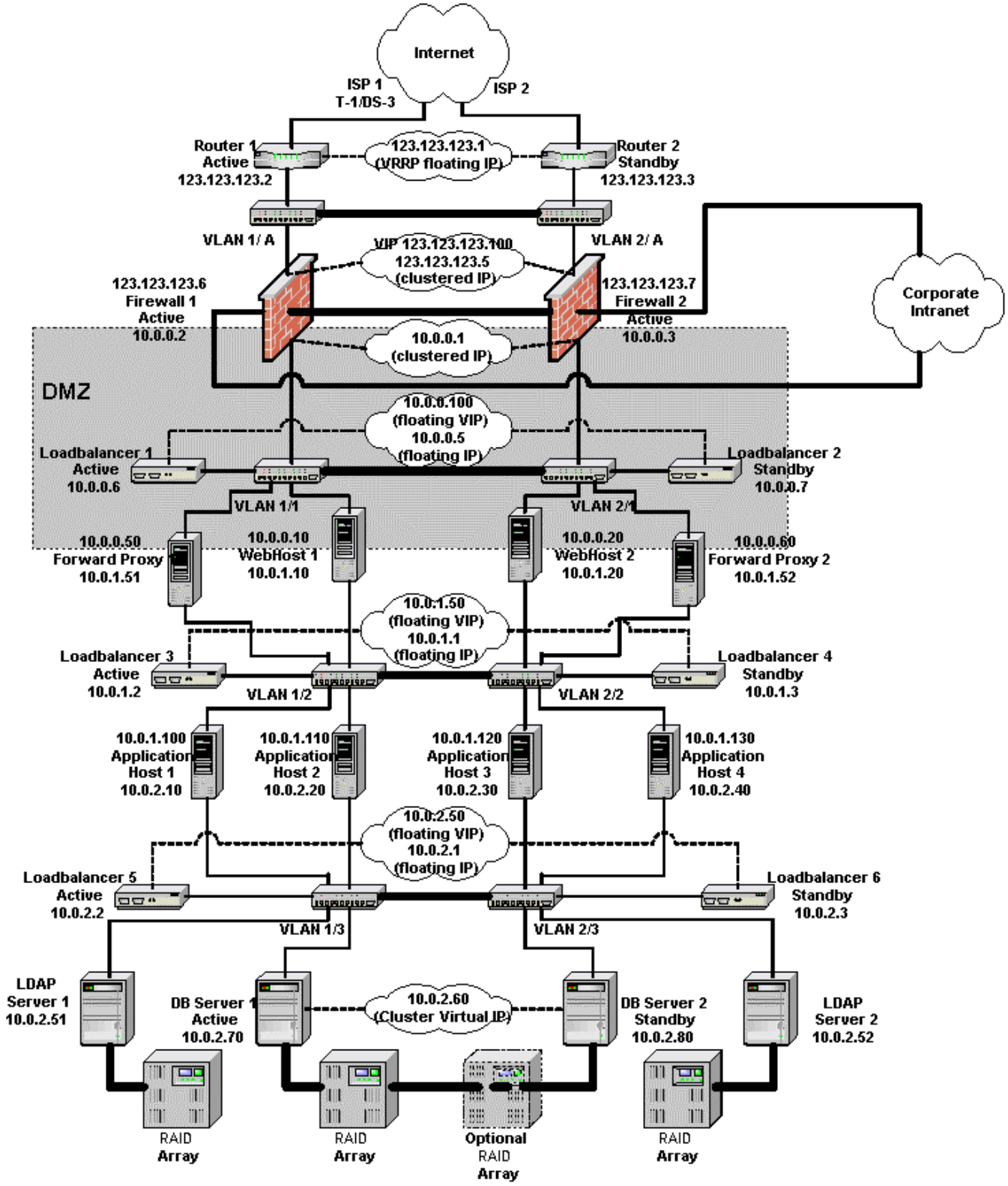
In the NAT DMZ architecture, the DMZ occupies a private and non-routable (RFC 1918) internet address space. The web servers are placed in this private address space in the DMZ. NAT is performed by the firewalls 1 and 2. The load balancers route packets to the web servers on the same network. This configuration can be used only if the DMZ is not shared with non-NATable services, such as IPSec and Kerberos. If these non-NATable services must exist on the DMZ, the Publicly Addressed DMZ architecture from the next section must be used.

Physical Layout

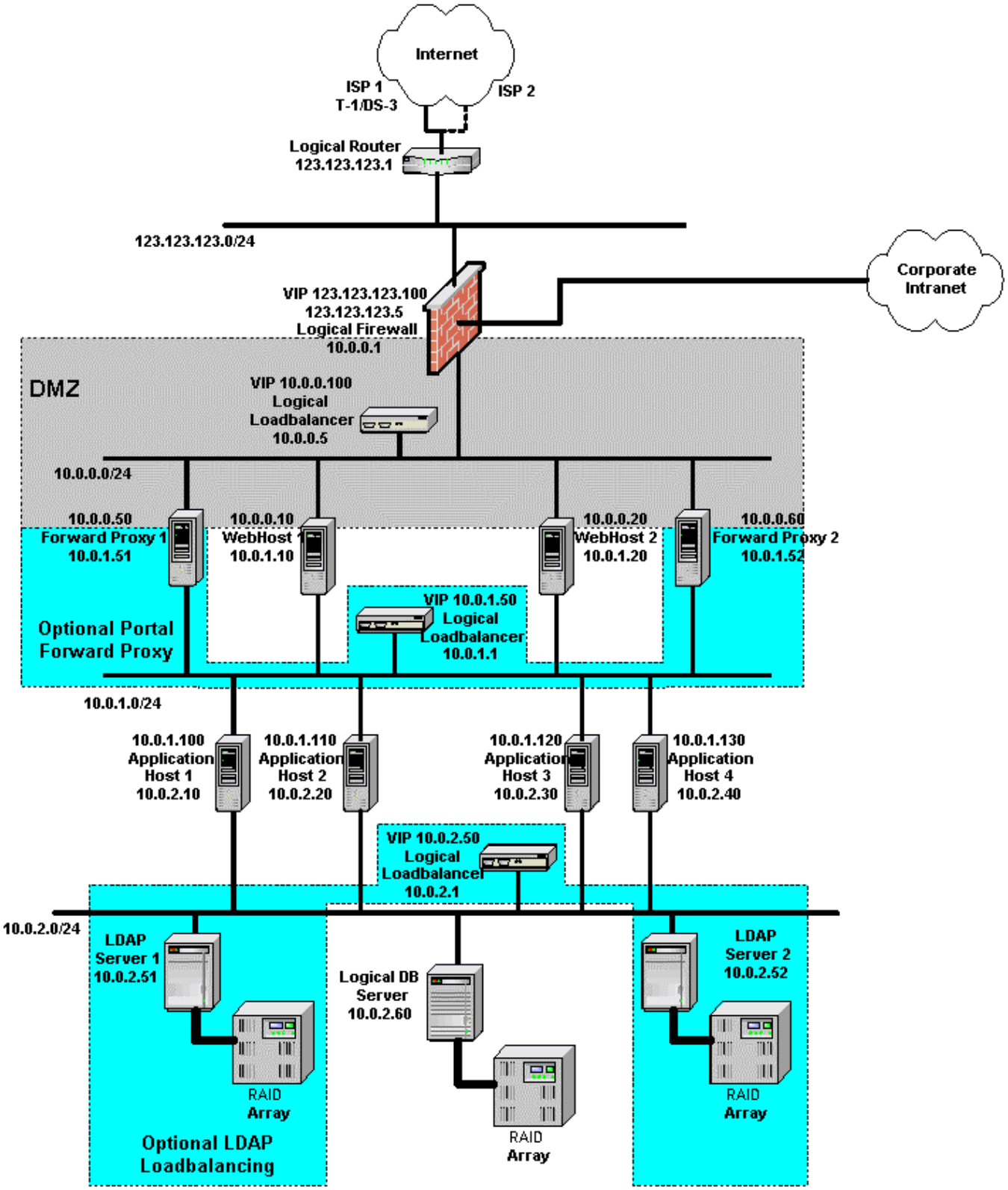
The following diagram includes these elements:

- Redundant ISP provider connections for high availability.
- Redundant routers 1 and 2 to connect to the internet.
- Redundant 3 prong firewalls 1 and 2 to perform NAT and connect the corporate network to the DMZ.
- Redundant load balancers 1 and 2 to load-balance requests to web servers 1 and 2.
- Redundant load balancers 3 and 4 used to load-balance outbound PIA requests to forward proxies 1 and 2.
- Web servers 1 and 2 that communicate to application servers 1 through 4.
- Application servers 1 through 4 optionally could use load balancers 5 and 6 to communicate to LDAP servers 1 and 2 for PIA authentication.
- LDAP servers 1 and 2 each has its own RAID storage for fault tolerance.
- Application servers 1 through 4 communicate with a clustered database server 1(2).
- Clustered database servers 1 and 2 share RAID storage for fault tolerance.

Physical Layout (cont'd)



Logical Layout



Router Setup

Unit	Router 1 (Active)	Router 2 (Standby)
IP Address	123.123.123.2	123.123.123.3
Subnet Mask	255.255.255.0	255.255.255.0
Packet filters (only if available)	Allow only HTTP/HTTPS to the PeopleSoft system. If the PeopleSoft portal is to call outside, then allow HTTP/HTTPS to outside from the PeopleSoft system. Allow rules as needed by other non-PeopleSoft systems.	Same as Unit 1.

Firewall Setup

Unit	Firewall 1 (Active)	Firewall 2 (Active)
IP Address 1	123.123.123.6	123.123.123.7
Subnet Mask 1	255.255.255.0	255.255.255.0
Shared Address 1	123.123.123.5	123.123.123.5
Default Route 1	123.123.123.1	123.123.123.1
IP Address 2	10.0.0.2	10.0.0.3
Subnet Mask 2	255.255.255.0	255.255.255.0
Shared Address 2	10.0.0.1	10.0.0.1
Default Route 2	None	None
IP Address 3	*	*
Subnet Mask 3	*	*
Shared Address 3	*	*
Default Route 3	None	None

* Based on the intranet IP address, it can be RFC 1918 address space.

Note. Both firewall units have the same security setup.

Access to PIA/Portal from Outside

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	Any	80	123.123.123.100	80	Allow
HTTPS	TCP	Any	443	123.123.123.100	443	Allow

Access to Outside from Portal/Application Messaging Service

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	10.0.0.50	Any	Any	Any	Allow
HTTPS	TCP	10.0.0.50	Any	Any	Any	Allow

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	10.0.0.60	Any	Any	Any	Allow
HTTPS	TCP	10.0.0.60	Any	Any	Any	Allow

Access to Provider's DNS Server from Local DNS Server

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
DNS1	UDP	Local DNS	Any	Provider's DNS	53	Allow
DNS1	TCP	Local DNS	Any	Provider's DNS	53	Allow

[1] Do not allow the reverse path. For example, do not allow the provider's DNS updates to reach local DNS

Static Address Mapping for Inbound Firewall NAT

External IP Address	Transport Protocol	External Port	Internal Address	Internal Port
123.123.123.100	TCP	80	10.0.0.100	80
123.123.123.100	TCP	443	10.0.0.100	443

Static Address Mapping for Outbound Firewall Reverse NAT

Source IP	Transport Protocol	Source Port	Translated IP	Translated Port
10.0.0.50	TCP	Any	123.123.123.50	Any
10.0.0.60	TCP	Any	123.123.123.60	Any

Web Server Load Balancer Setup

Unit	Load Balancer 1 (Active)	Load Balancer 2 (Standby)
IP Address	10.0.0.6	10.0.0.7
Subnet Mask	255.255.255.0	255.255.255.0
Shared Address	10.0.0.5	10.0.0.5
Default Route	10.0.0.1	10.0.0.1
Virtual IP (portal.corp.com)	10.0.0.100	10.0.0.100
HTTP Service Port	80	80
HTTPS Service Port	443	443
HTTP Persistence (sticky)	Load balancer cookie	Load balancer cookie
HTTPS Persistence (sticky)	Load balancer SSL sticky	Load balancer SSL sticky

Web Server Setup

The configuration parameters vary based on the web server clustering scheme that you select. Refer to the *Clustering and High Availability of PeopleSoft 8.4* red paper available on Customer Connection for more information.

Unit	WebHost1:Instance1	WebHost1:Instance2	WebHost2:Instance1	WebHost2:Instance2
IP Address 1	*	*	*	*
Subnet Mask 1	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Unit	WebHost1:Instance1	WebHost1:Instance2	WebHost2:Instance1	WebHost2:Instance2
Default Route 1	10.0.0.5	10.0.0.5	10.0.0.5	10.0.0.5
HTTP Port	*	*	*	*
HTTPS Port	*	*	*	*
IP Address 2	10.0.1.10	10.0.1.10	10.0.1.20	10.0.1.20
Subnet Mask 2	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default Route 21	10.0.1.50	10.0.1.50	10.0.1.50	10.0.1.50

* See the *Clustering and High Availability of PeopleSoft 8.4* red paper available on Customer Connection for values.[1] Set to none if proxy load balancing is not used

Forward Proxy Setup

This is an optional setup for Portal, Application Messaging, and Business Interlinks outbound calls.

Unit	ForwardProxy1	ForwardProxy2
IP Address 1	10.0.0.50	10.0.0.60
Subnet Mask 1	255.255.255.0	255.255.255.0
Default Route 1	10.0.0.1	10.0.0.1
IP Address 2	10.0.1.51	10.0.1.52
Subnet Mask 2	255.255.255.0	255.255.255.0
Default Route 2	10.0.0.50	10.0.0.60
HTTP Port	80	80
HTTPS Port	443	443

Forward Proxy Load Balancer Setup

This is an optional setup for Portal, Application Messaging, and Business Interlinks outbound calls.

Unit	Load Balancer 3 (Active)	Load Balancer 4 (Standby)
IP Address	10.0.1.2	10.0.1.3
Subnet Mask	255.255.255.0	255.255.255.0
Shared Address	10.0.1.1	10.0.1.1
Default Route	None	None
Virtual IP for Proxy Service	10.0.1.50	10.0.1.50
HTTP Service Port	80	80
HTTPS Service Port	443	443
Persistence (sticky)	IP Based	IP Based

Application Server Setup

Unit	AppHost1:Domain1	AppHost1:Domain2	AppHost2:Domain1	AppHost2:Domain2
IP Address 1	10.0.1.100	10.0.1.100	10.0.1.110	10.0.1.110
Subnet Mask 1	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Unit	AppHost1:Domain1	AppHost1:Domain2	AppHost2:Domain1	AppHost2:Domain2
Default Route 1	10.0.0.1	10.0.0.1	10.0.0.1	10.0.0.1
JSH Port	9000	9020	9000	9020
IP Address 2	10.0.2.10	10.0.2.10	10.0.2.20	10.0.2.20
Subnet Mask 2	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default Route 1	10.0.0.5	10.0.0.5	10.0.0.5	10.0.0.5
LDAP Host	10.0.2.50	10.0.2.50	10.0.2.50	10.0.2.50
LDAP Port	389	389	389	389
LDAPS Port	636	636	636	636

LDAP Load Balancer Setup

This is an optional setup for LDAP load balancing.

Unit	Load Balancer 5 (Active)	Load Balancer 6 (Standby)
IP Address	10.0.2.2	10.0.2.3
Subnet Mask	255.255.255.0	255.255.255.0
Shared Address	10.0.2.1	10.0.2.1
Default Route	None	None
Virtual IP for Proxy Service	10.0.2.50	10.0.2.50
LDAP Service Port	389	389
LDAPS Service Port	636	636
Persistence (sticky)	IP Based	IP Based

Database Server Setup

Unit	DBServer1	DBServer2
IP Address	10.0.2.70	10.0.2.80
Subnet Mask	255.255.255.0	255.255.255.0
Default Route	None	None
Service VIP1	10.0.2.60	10.0.2.60
Service Port	DB Vendor Specific	DB Vendor Specific

[1] Required only if database is clustered.

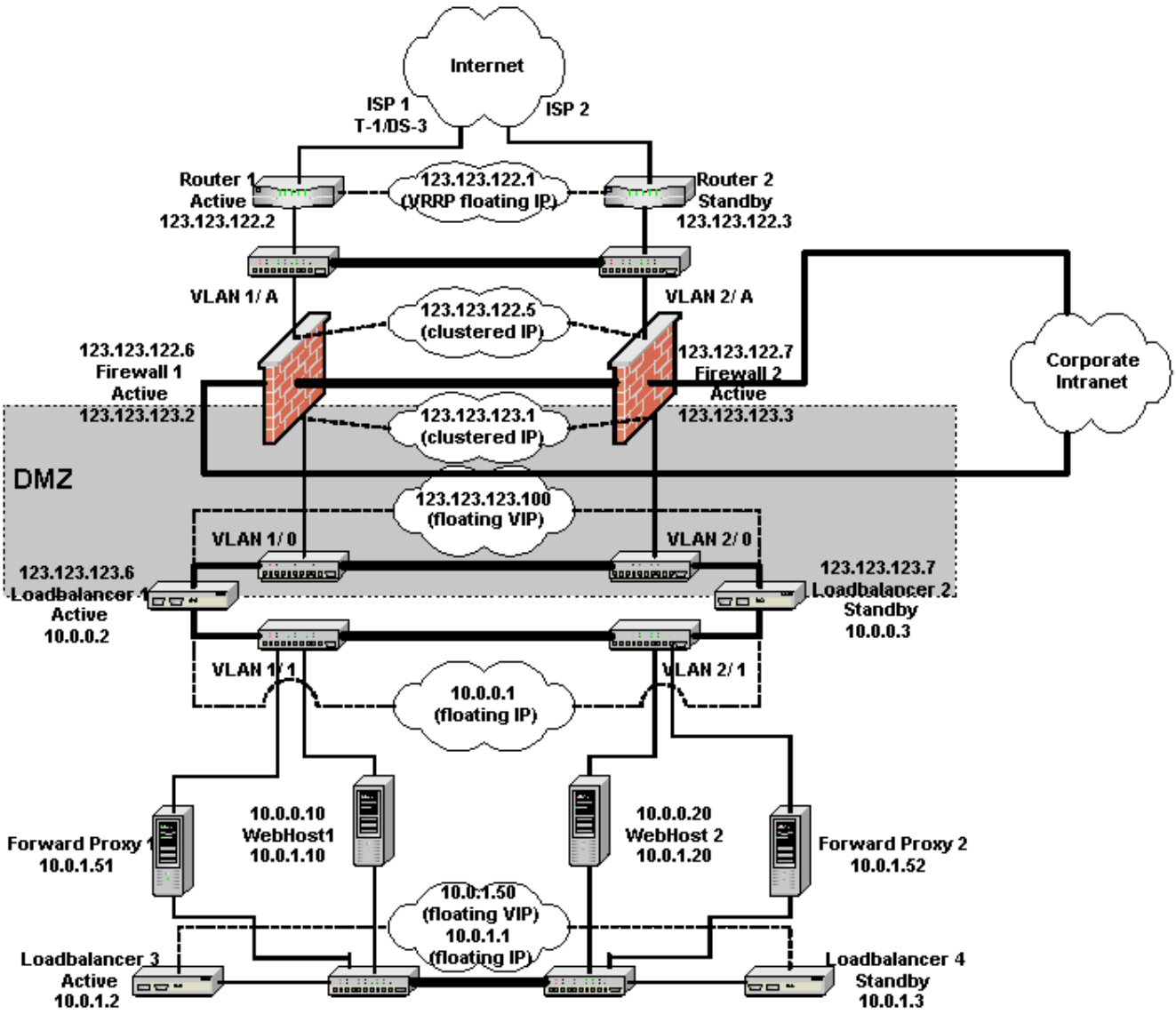
Publicly Addressed DMZ Infrastructure

In this architecture, the DMZ occupies a publicly addressable IP address space. The load balancers perform NAT and pass packets to the web servers that reside in a private and non-routable (RFC 1918) internet address space. This configuration should be used if the DMZ has to be shared with non-NATable services, such as IPSec and Kerberos. The following diagram shows only the modified portion of the infrastructure. The application and database servers in the infrastructure are the same as the NAT DMZ infrastructure and have not been shown. .

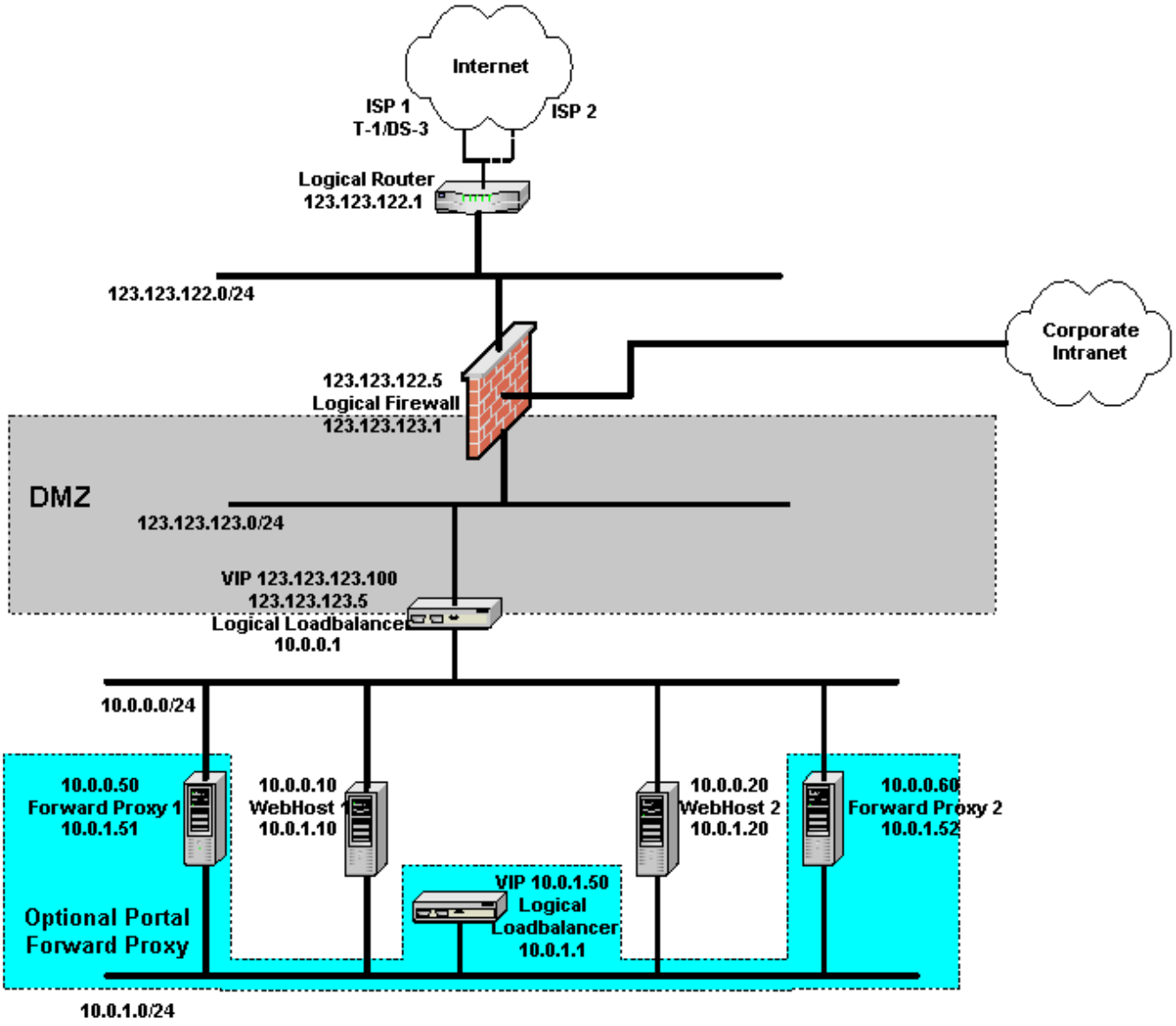
Physical Layout

The following diagram includes these elements:

- A redundant ISP provider connection for high availability.
- Redundant routers 1 and 2 to connect to the internet.
- Redundant three-prong firewalls 1 and 2 to connect the corporate network to the DMZ.
- Redundant load balancers 1 and 2 to perform NAT and load-balance requests to web servers 1 and 2.
- Redundant load balancers 3 and 4 to load-balance outbound PIA requests to forward proxy servers 1 and 2.
- Web servers 1 and 2, which communicate to application servers not shown in the diagram.



Logical Layout



Router Setup

Unit	Router 1 (Active)	Router 2 (Standby)
IP Address	123.123.122.2	123.123.122.3
Subnet Mask	255.255.255.0	255.255.255.0
Packet filters (only if available)	Allow only HTTP/HTTPS to the PeopleSoft system. If the PeopleSoft portal is to call outside, allow HTTP/HTTPS to outside from the PeopleSoft system. Allow rules as needed by other non-PeopleSoft systems.	Same as Unit 1.

Firewall Setup

Unit	Firewall 1 (Active)	Firewall 2 (Active)
IP Address 1	123.123.122.6	123.123.122.7
Subnet Mask 1	255.255.255.0	255.255.255.0
Shared Address 1	123.123.122.5	123.123.122.5
Default Route 1	123.123.122.1	123.123.122.1
IP Address 2	123.123.123.2	123.123.123.3
Subnet Mask 2	255.255.255.0	255.255.255.0
Shared Address 2	123.123.123.1	123.123.123.1
Default Route 2	None	None
IP Address 3	*	*
Subnet Mask 3	*	*
Shared Address 3	*	*
Default Route 3	None	None

* Based on the intranet IP address, it can be the RFC 1918 address space.

Note. Both firewall units have the same security setup.

Access to PIA/Portal from Outside

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	Any	80	123.123.123.100	80	Allow
HTTPS	TCP	Any	443	123.123.123.100	443	Allow

Access to Outside from Portal/Application Messaging Service

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	123.123.123.50	Any	Any	Any	Allow
HTTPS	TCP	123.123.123.50	Any	Any	Any	Allow
HTTP	TCP	123.123.123.60	Any	Any	Any	Allow
HTTPS	TCP	123.123.123.60	Any	Any	Any	Allow

Access to Provider's DNS Server from Local DNS Server

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
DNS1	UDP	Local DNS	Any	Provider's DNS	53	Allow
DNS1	TCP	Local DNS	Any	Provider's DNS	53	Allow

[1] Do not allow the reverse path. For example, do not allow the provider's DNS updates to reach the local DNS.

Web Server Load Balancer Setup

Unit	Load Balancer 1 (Active)	Load Balancer 2 (Standby)
IP Address (VLAN1/0)	123.123.123.6	123.123.123.7
Subnet Mask	255.255.255.0	255.255.255.0
Shared Address	123.123.123.5	123.123.123.5
Default Route	123.123.123.1	123.123.123.1
IP Address (VLAN1/1)	10.0.0.2	10.0.0.3
Subnet Mask	255.255.255.0	255.255.255.0
Shared Address	10.0.0.1	10.0.0.1
Virtual IP (portal.corp.com)	123.123.123.100	123.123.123.100
HTTP Service Port	80	80
HTTPS Service Port	443	443
HTTP Persistence (sticky)	Load Balancer Cookie	Load Balancer Cookie
HTTPS Persistence (sticky)	Load Balancer SSL Sticky	Load Balancer SSL Sticky

Static Address Mapping for Inbound Load Balancer NAT

External IP Address	Transport Protocol	External Port	Internal Address	Internal Port
123.123.123.100	TCP	80	10.0.0.100	80
123.123.123.100	TCP	443	10.0.0.100	443

Static Address Mapping for Outbound Load Balancer Reverse NAT

Source IP	Transport Protocol	Source Port	Translated IP	Translated Port
10.0.0.50	TCP	Any	123.123.123.50	Any
10.0.0.60	TCP	Any	123.123.123.60	Any

Web Server Setup

The configuration parameters vary based on the web server clustering scheme selected.

Unit	WebHost1:Instance1	WebHost1:Instance2	WebHost2:Instance1	WebHost2:Instance2
IP Address 1	*	*	*	*
Subnet Mask 1	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default Route 1	10.0.0.1	10.0.0.1	10.0.0.1	10.0.0.1
HTTP Port	*	*	*	*
HTTPS Port	*	*	*	*
IP Address 2	10.0.1.10	10.0.1.10	10.0.1.20	10.0.1.20
Subnet Mask 2	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
DefaultRoute 21	10.0.1.50	10.0.1.50	10.0.1.50	10.0.1.50

* See *Clustering and High Availability of PeopleSoft 8.4* red paper available on Customer Connection for values.[1] Set to none if proxy load balancing is not used.

Additional Security DMZ

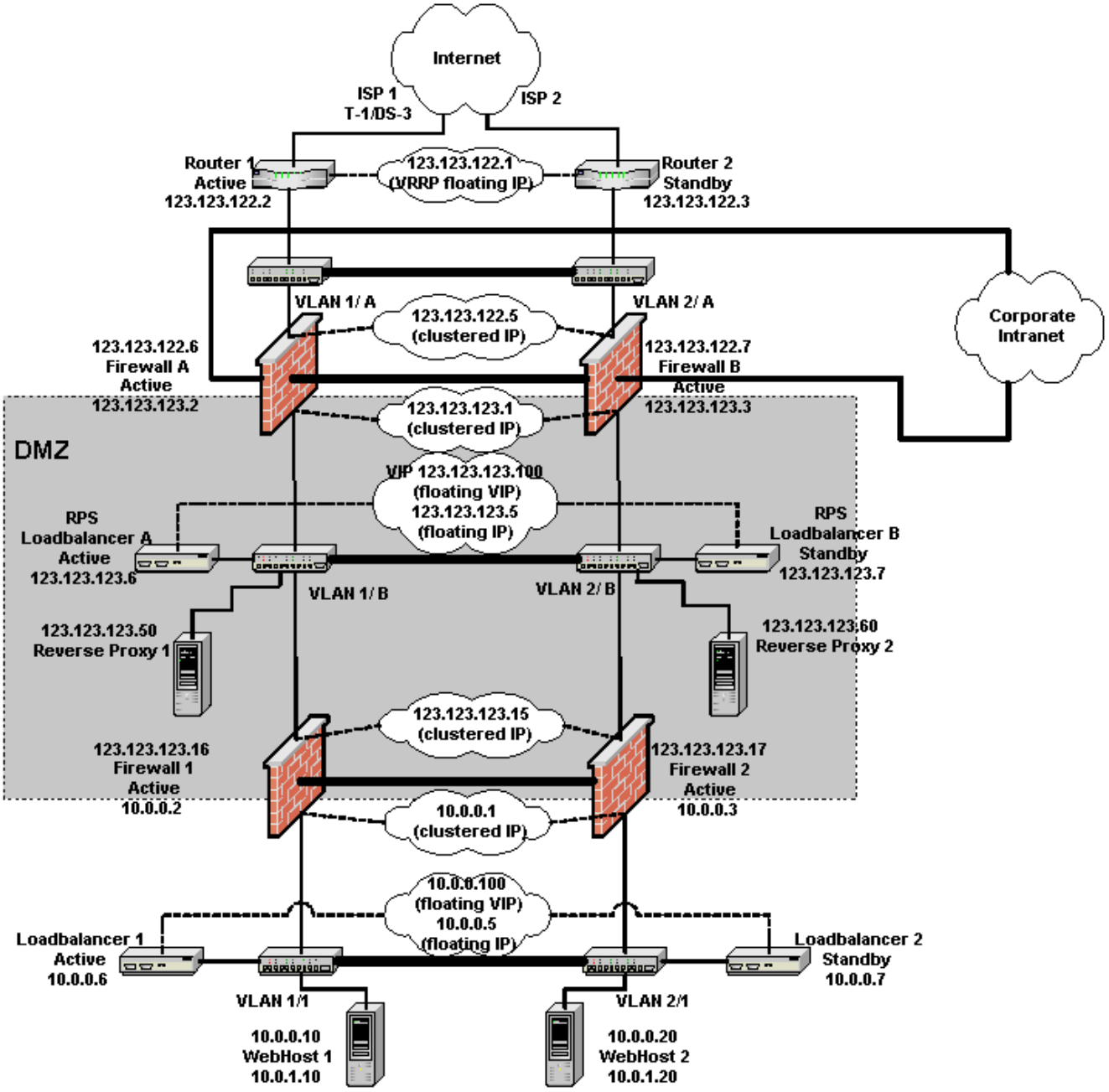
For a DMZ with higher security, use an architecture that consists of an outside firewall, an inside firewall, and a reverse proxy server (RPS). Ideally, the firewalls should be of a different model or made to maintain diversity in the architecture. The inside firewalls should allow only HTTP/HTTPS requests to originate from the RPS and terminate on the web servers. Requests from use to the RPS are loadbalanced by RPS Loadbalancer A(B) and requests from the RPS to webservers are loadbalanced by Loadbalancer 1(2). The rest of the setup from webserver onwards is the same as the ones described earlier.

Physical Layout

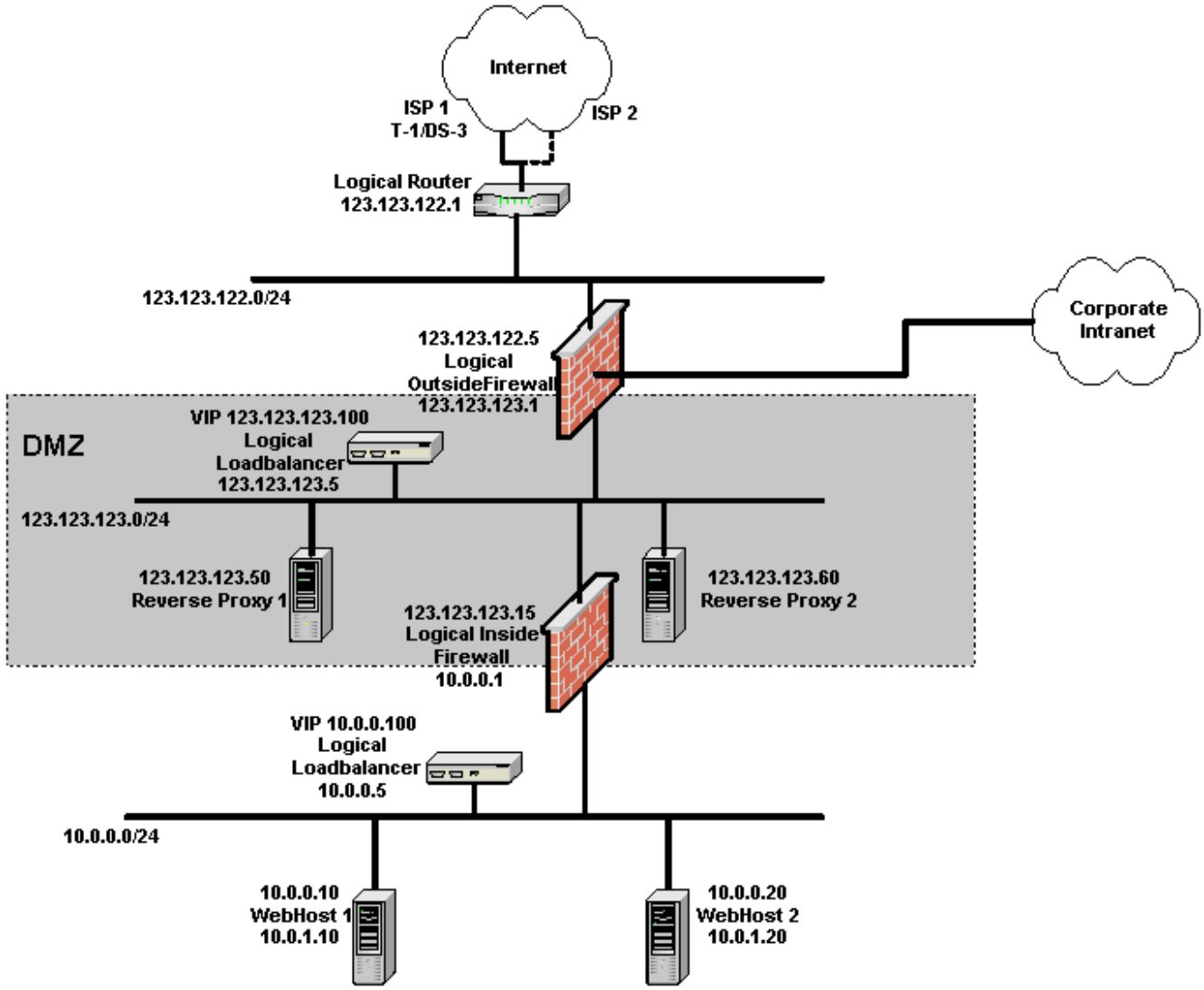
The following diagram includes these elements:

- Redundant ISP provider connection for high availability.
- Redundant routers 1 and 2 to connect to the internet.
- Redundant three-prong outside firewalls A and B to perform NAT, and connect the corporate network to the DMZ.
- Redundant load balancers A and B to load-balance requests to RPSs 1 and 2.
- Redundant inside firewalls 1 and 2 that provide additional security by moving web servers 1 and 2 away from the DMZ.
- Redundant load balancers 1 and 2 that load-balance requests from RPSs 1 and 2 to web servers 1 and 2.
- Web servers 1 and 2 that communicate to application servers and forward proxy servers not shown in the diagram.

Physical Layout (cont'd)



Logical Layout



Router Setup

Unit	Router 1 (Active)	Router 2 (Standby)
IP Address	123.123.122.2	123.123.122.3
Subnet Mask	255.255.255.0	255.255.255.0
VRRP IP Address	123.123.122.1	123.123.122.1
VRRP Priority	200	100
Packet filters (only if available)	Allow only HTTP/HTTPS to the PeopleSoft system. If the PeopleSoft portal is to call outside, allow HTTP/HTTPS to outside from the PeopleSoft system. Allow rules as needed by other non-PeopleSoft systems.	Same as Unit 1.

Outside Firewall Setup

Unit	Firewall A (Active)	Firewall B (Active)
IP Address 1	123.123.122.6	123.123.122.7
Subnet Mask 1	255.255.255.0	255.255.255.0
Shared Address 1	123.123.122.5	123.123.122.5
Default Route 1	123.123.122.1	123.123.122.1
IP Address 2	123.123.123.2	123.123.123.3
Subnet Mask 2	255.255.255.0	255.255.255.0
Shared Address 2	123.123.123.1	123.123.123.1
Default Route 2	None	None
IP Address 3	*	*
Subnet Mask 3	*	*
Shared Address 3	*	*
Default Route 3	None	None

* Based on the intranet IP address, it can be the RFC 1918 address space.

Note. Both firewall units have the same security setup.

Access to PIA/Portal from Outside

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	Any	80	123.123.123.100	80	Allow
HTTPS	TCP	Any	443	123.123.123.100	443	Allow

Access to Outside from Portal/Application Messaging Service

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	123.123.123.50	Any	Any	Any	Allow
HTTPS	TCP	123.123.123.50	Any	Any	Any	Allow
HTTP	TCP	123.123.123.60	Any	Any	Any	Allow
HTTPS	TCP	123.123.123.60	Any	Any	Any	Allow

Access to Provider's DNS Server from Local DNS Server

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
DNS1	UDP	Local DNS	Any	Provider's DNS	53	Allow
DNS1	TCP	Local DNS	Any	Provider's DNS	53	Allow

[1] Do not allow the reverse path. For example, do not allow a provider's DNS updates to reach the local DNS.

Reverse Proxy Server Load Balancer Setup

Unit	Load Balancer A (Active)	Load Balancer B (Standby)
IP Address	123.123.123.6	123.123.123.7
Subnet Mask	255.255.255.0	255.255.255.0
Shared Address	123.123.123.5	123.123.123.5
Default Route	123.123.123.1	123.123.123.1
Virtual IP (portal.corp.com)	123.123.123.100	123.123.123.100
HTTP Service Port	80	80
HTTPS Service Port	443	443
HTTP Persistence (sticky)	Load Balancer Cookie	Load Balancer Cookie
HTTPS Persistence (sticky)	Load Balancer SSL Sticky	Load Balancer SSL Sticky

Reverse Proxy Server Setup

Unit	RPS1	RPS2
IP Address 1	123.123.123.50	123.123.123.60
Subnet Mask 1	255.255.255.0	255.255.255.0
Default Route 1	123.123.123.5	123.123.123.5
HTTP Port	80	80
HTTPS Port	443	443

Inside Firewall Setup

Unit	Firewall 1 (Active)	Firewall 2 (Active)
IP Address 1	123.123.123.16	123.123.123.17
Subnet Mask 1	255.255.255.0	255.255.255.0
Shared Address 1	123.123.123.15	123.123.123.15
Default Route 1	123.123.123.1	123.123.123.1
IP Address 2	10.0.0.2	10.0.0.3
Subnet Mask 2	255.255.255.0	255.255.255.0
Shared Address 2	10.0.0.1	10.0.0.1
Default Route 2	None	None

Note. Both firewall units have the same security setup.

Access to PIA/Portal from RPS Only

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	123.123.123.50	80	10.0.0.100	80	Allow
HTTPS	TCP	123.123.123.50	443	10.0.0.100	443	Allow

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	123.123.123.60	80	10.0.0.100	80	Allow
HTTPS	TCP	123.123.123.60	443	10.0.0.100	443	Allow

Access to Outside from Portal/Application Messaging Service

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	10.0.0.50	Any	Any	Any	Allow
HTTPS	TCP	10.0.0.50	Any	Any	Any	Allow
HTTP	TCP	10.0.0.60	Any	Any	Any	Allow
HTTPS	TCP	10.0.0.60	Any	Any	Any	Allow

Static Address Mapping on Inside Firewall for Inbound NAT

External IP Address	Transport Protocol	External Port	Internal Address	Internal Port
123.123.123.100	TCP	80	10.0.0.100	80
123.123.123.100	TCP	443	10.0.0.100	443

Static Address Mapping on Inside Firewall for Outbound Reverse NAT

Source IP	Transport Protocol	Source Port	Translated IP	Translated Port
10.0.0.50	TCP	Any	123.123.123.50	Any
10.0.0.60	TCP	Any	123.123.123.60	Any

Web Server Load Balancer Setup

Unit	Load Balancer 1 (Active)	Load Balancer 2 (Standby)
IP Address	10.0.0.6	10.0.0.7
Subnet Mask	255.255.255.0	255.255.255.0
Shared Address	10.0.0.5	10.0.0.5
Default Route	10.0.0.1	10.0.0.1
Virtual IP (portal.corp.com)	10.0.0.100	10.0.0.100
HTTP Service Port	80	80
HTTPS Service Port	443	443
HTTP Persistence (sticky)	Load Balancer Cookie	Load Balancer Cookie
HTTPS Persistence (sticky)	Load Balancer SSL Sticky	Load Balancer SSL Sticky

Web Server Setup

All other setup, including web server setup, is the same as the NAT DMZ configuration.

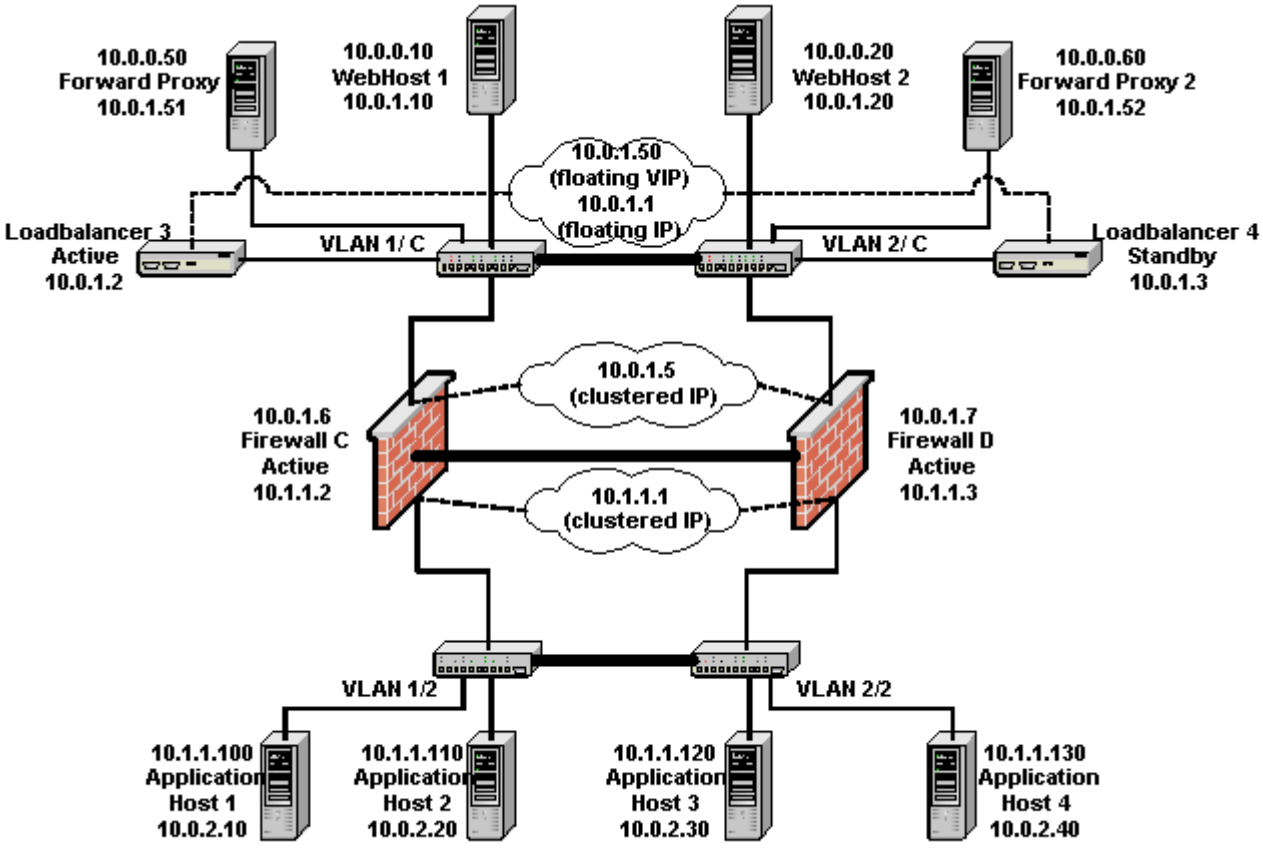
Firewall Application Server

After the web server has been adequately secured by one of the setups described earlier, a firewall can be used between the web server and the application server for additional security. In this setup, firewalls C and D are added for this purpose. The new firewall policies allow JOLT requests to originate from the web servers only. Additionally, all outbound requests to the forward proxy server are limited to HTTP/HTTPS and can only originate from one of the application servers. No other outbound/inbound requests are allowed.

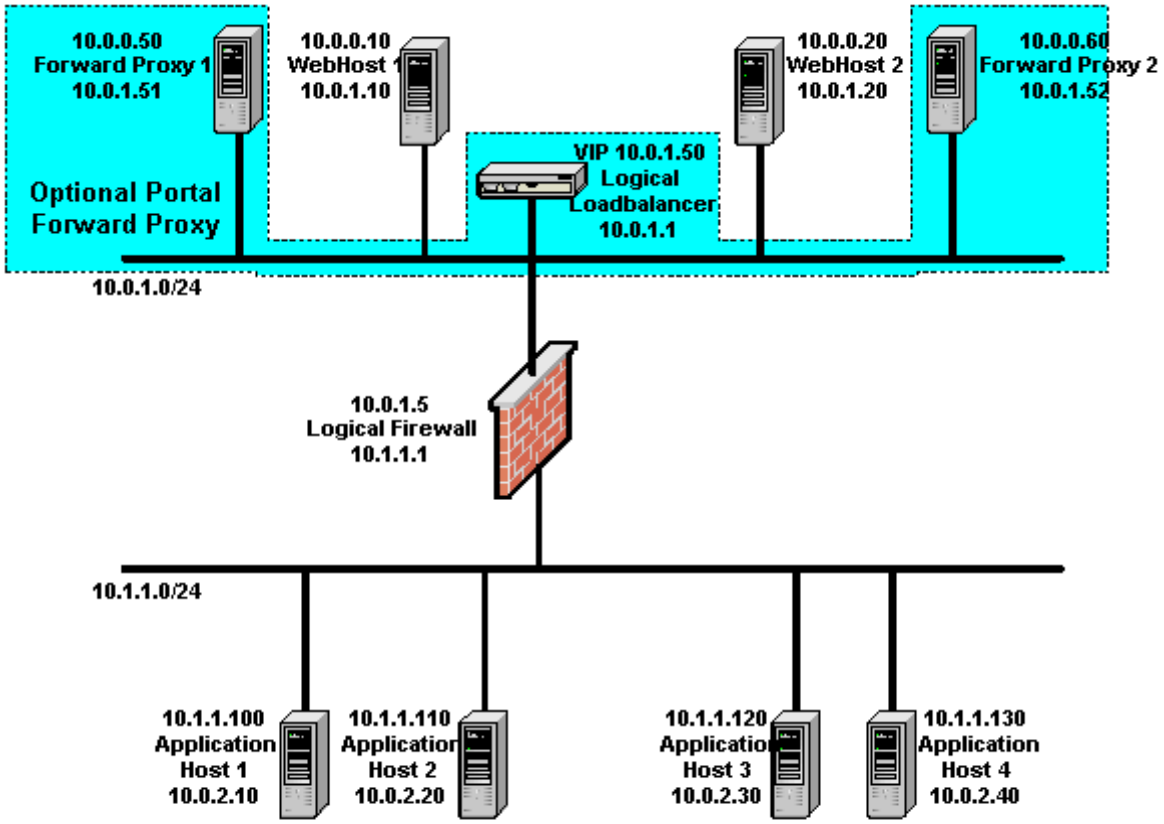
Physical Layout

The following diagram includes these elements:

- Additional infrastructure to communicate to web servers 1 and 2 not shown in the diagram.
- Redundant inside firewalls C and D that provide additional security by separating application servers 1 through 4 from web servers 1 and 2.
- Load balancers 3 and 4 load-balance requests from application servers 1 through 4 to forward proxy servers 1 and 2 via inside firewalls C and D.
- Application servers 1 through 4 communicate to database servers not shown in the diagram.



Logical Layout



Application Server Firewall Setup

Unit	Firewall C (Active)	Firewall D (Active)
IP Address 1	10.0.1.6	10.0.1.7
Subnet Mask 1	255.255.255.0	255.255.255.0
Shared Address 1	10.0.1.5	10.0.1.5
Default Route 1	10.0.1.11	10.0.1.11
IP Address 2	10.1.1.2	10.1.1.3
Subnet Mask 2	255.255.255.0	255.255.255.0
Shared Address 2	10.1.1.1	10.1.1.1
Default Route 2	None	None

Access to Application Server from Web Server Only

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
JOLT	TCP	10.0.1.10	Any	10.1.1.100	*	Allow
JOLT	TCP	10.0.1.20	Any	10.1.1.100	*	Allow

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
JOLT	TCP	10.0.1.10	Any	10.1.1.110	*	Allow
JOLT	TCP	10.0.1.20	Any	10.1.1.110	*	Allow
JOLT	TCP	10.0.1.10	Any	10.1.1.120	*	Allow
JOLT	TCP	10.0.1.20	Any	10.1.1.120	*	Allow
JOLT	TCP	10.0.1.10	Any	10.1.1.130	*	Allow
JOLT	TCP	10.0.1.20	Any	10.1.1.130	*	Allow

* This is a port range starting from the JOLT listener port number up to the total number of handlers. For example, if the JOLT listener is 9000 and 5 JOLT handlers exist, the port range to allow is 9000–9005. If a JOLT relay is used, then allow the JOLT relay port rather than the port range for each server.

Access to Outside from Application Messaging Service

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	10.1.1.100	Any	10.0.1.50	Proxy HTTP Port (7080)	Allow
HTTPS	TCP	10.1.1.100	Any	10.0.1.50	Proxy HTTPS Port (7443)	Allow
HTTP	TCP	10.1.1.110	Any	10.0.1.50	Proxy HTTP Port (7080)	Allow
HTTPS	TCP	10.1.1.110	Any	10.0.1.50	Proxy HTTPS Port (7443)	Allow
HTTP	TCP	10.1.1.120	Any	10.0.1.50	Proxy HTTP Port (7080)	Allow
HTTPS	TCP	10.1.1.120	Any	10.0.1.50	Proxy HTTPS Port (7443)	Allow
HTTP	TCP	10.1.1.130	Any	10.0.1.50	Proxy HTTP Port (7080)	Allow
HTTPS	TCP	10.1.1.130	Any	10.0.1.50	Proxy HTTPS Port (7443)	Allow
HTTP	TCP	10.1.1.140	Any	10.0.1.50	Proxy HTTP Port (7080)	Allow
HTTPS	TCP	10.1.1.140	Any	10.0.1.50	Proxy HTTPS Port (7443)	Allow

ADDITIONAL NETWORK PROTECTION

Here we describe additional hardware protection, for instance, Intrusion Detection and Prevention Systems and Web Application Firewalls. Many sources for information on Intrusion Detection and Prevention Systems and Web Application Firewalls are available. The information here has been sourced from Wikipedia.

Intrusion Detection Systems

An intrusion detection system (IDS) is a device (or application) that monitors network activities, system activities, or both for malicious activities or policy violations and produces reports to a management station. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization.

IDPSs typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSs can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (for example, reconfiguring a firewall), or changing the attack's content.

Passive System versus Reactive System

In a passive system, the intrusion detection system (IDS) sensor detects a potential security breach, logs the information, and signals an alert on the console and or owner. In a reactive system, also known as an intrusion prevention system (IPS), the IPS responds to the suspicious activity by resetting the connection or by reprogramming the firewall to block network traffic from the suspected malicious source. This can happen automatically or at the command of an operator.in reactive intrusion detection system is one in which if the intruder or attacks are detected, it does not alert the user but rather responds to the illegal activity for shows a strict reaction.

Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators.

Intrusion Prevention Systems

An IPS is typically designed to operate completely invisibly on a network. IPS products do not typically claim an IP address on the protected network but may respond directly to any traffic in a variety of ways. (Common IPS responses include dropping packets, reseting connections, generating alerts, and even quarantining intruders.) While some IPS products can implement firewall rules, this is often a mere convenience and not a core function of the product. Moreover, IPS technology offers deeper insight into network operations providing information about overly active hosts, bad logons, inappropriate content, and many other network and application layer functions.

Application firewalls are a very different type of technology. An application firewall uses proxies to perform firewall access control for network and application-layer traffic. Some application-layer firewalls can do some IPS-like functions, such as enforcing RFC specifications on network traffic. Also, some application layer firewalls have also integrated IPS-style signatures into their products to provide real-time analysis and blocking of traffic. Application firewalls do have IP addresses on their ports and are directly addressable. Moreover, they use full proxy features to decode and reassemble packets. Not all IPSs perform full proxy-like processing. Also, application-layer firewalls tend to focus on firewall capabilities, with IPS

capabilities as add-on. While numerous similarities between the two technologies exist, they are not identical and are not interchangeable.

Unified Threat Management (UTM), sometimes called *next generation firewalls,* are also a different breed of product entirely. UTM products bring together multiple security capabilities onto a single platform. A typical UTM platform provides firewall, VPN, antivirus, web filtering, intrusion prevention, and antispam capabilities. Some UTM appliances are derived from IPS products such as 3Com's X-series products. Others are derived from a combination with firewall products, such as Juniper's SSG or Cisco's Adaptive Security Appliances (ASA). And still others were derived from the ground up as a UTM appliance such as Netasq, SonicWALL, Fortinet, Calyptix, GajShield, and Astaro. The main feature of a UTM is that it includes multiple security features on one appliance. IPS is merely one feature.

Access control is an entirely different security concept. Access control refers to general rules allowing hosts, users, or applications access to specific parts of a network. Typically, access control helps organizations segment networks and limit access. While an IPS can block access to users, hosts, or applications, it does so only when malicious code has been discovered. As such, IPS does not necessarily serve as an access control device. While it has some access control abilities, firewalls and network access control (NAC) technologies are better suited to provide these features.

Web Application Firewalls

An application firewall is a form of firewall that controls any combination of input, output, and access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall. The application firewall is typically built to monitor one or more specific applications or services (such as a web or database service), unlike a stateful network firewall, which can provide some access controls for nearly any kind of network traffic. Two primary categories of application firewalls exist, network-based application firewalls and host-based application firewalls.

Application firewalls that are specific to a particular kind of network traffic may be titled with the service name, such as a web application firewall. They can be implemented through software running on a host or a standalone piece of network hardware. Often, it is a host using various forms of proxy servers to proxy traffic before passing it on to the client or server. Because it acts on the application layer, it may inspect the contents of the traffic, blocking specified content, such as certain websites and viruses, and it attempts to exploit known logical flaws in client software.

Network-based application-layer firewalls work on the application level of the network stack (for example, all web browser, telnet, or ftp traffic), and can intercept all packets traveling to or from an application. In principle, application firewalls can prevent all unwanted outside traffic from reaching protected machines.

Modern application firewalls can also offload encryption from servers, block application input and output from detected intrusions or malformed communication, manage or consolidate authentication, or block content that violates policies.

Oracle Adaptive Access Manager

Oracle Adaptive Access Manager provides superior protection for businesses and their customers through real-time fraud prevention, multifactor authentication, and unique authentication strengthening. Oracle Adaptive Access Manager consists of two primary components that together create one of the most powerful and flexible weapons in the war against fraud. Adaptive Strong Authenticator provides multifactor authentication and protection mechanisms for sensitive information such as passwords, PINs, security questions, account numbers, and other credentials.

Adaptive Risk Manager provides real-time and offline risk analysis and proactive actions to prevent fraud at critical login and transaction checkpoints. Adaptive Risk Manager examines and profiles a large number of contextual data points to dynamically determine the level of risk during each unique login and transaction attempt. Oracle Adaptive Access Manger strengthens and complements other identity and access management products such as single sign-on, federation, and fine-grained authorization with its unique security capabilities. Open frameworks and multiple deployment options ensure ease of integration for superior interoperability.

Chapter 4 - Securing PeopleSoft Internet Architecture

Once the infrastructure is secure, PeopleSoft Internet Architecture needs to be secured. The various layers to secure for a production system are described here followed by individual sections describing how to configure each item.

- Apply vendor-recommended security-hardening procedure to the web server.
- Use HTTPS as a minimum level of security for PeopleSoft Internet Architecture.
- Disable HTTP access to PeopleSoft Internet Architecture, if possible.
- Change default password of PSKEY.
- Disable configuration re-initialization.
- Disable browser caching for applications deployed in a kiosk environment.

Note: If you deploy Microsoft Windows workstations as kiosks in common areas for facilitating access to sensitive personal information, such as payslips, and you don't require individual network login for access to these workstations, we strongly recommend that you consider deploying robust kiosk software, for instance http://faronics.com/en/Products/DeepFreeze/DeepFreezeHospitality.aspx.

- Use a forward proxy server for the portal and integration gateway when using a firewall.
- Configure the forward proxy to bypass local addresses.
- Use only HTTPS and mutual authentication for integration.
- Use FTPS (or SFTP when available) instead of FTP.
- Encrypt the password in the integration.properties file.
- Use secure LDAP (LDAPS) for authentication.
- If possible, disable anonymous BIND on LDAP.
- Use TUXEDO layer encryption.
- If using the Oracle database, use ASO encryption to connect to the database.

How to Security Harden the Web Server

WebLogic

If you have deployed an Oracle WebLogic J2EE server, take the following steps to harden the installation:

- Follow Oracle's recommendations for hardening WebLogic, located on the Oracle website at http://download.oracle.com/docs/cd/E14571_01/wls.htm

Scroll down to: Security > Securing a Production Environment > Ensuring the Security of Your Production Environment > Securing the WebLogic Server Host

- Change the WebLogic server user's password.
  Follow the instructions in Enterprise PeopleTools PeopleBook: System and Server Administration, "Working with Oracle WebLogic," Changing a WebLogic User's Password.
- Restrict access to a servlet.
  Follow the instructions in *Enterprise PeopleTools PeopleBook: System and Server Administration,* "Working with Oracle WebLogic," Restricting Access to a Servlet.

WebSphere

If you have deployed a WebSphere J2EE server, follow the IBM recommendations to security harden the installation, located on the IBM website at http://publib-b.boulder.ibm.com/abstracts/sg246451.html?Open

How to Enable SSL on a Web Server for HTTPS

Please refer to PeopleBooks for instructions on how to enable SSL on the web server.

See http://www.oracle.com/pls/psft/homepage

WebLogic

Follow the instructions in *Enterprise PeopleTools PeopleBook: System and Server Administration,* "Working with Oracle WebLogic," Defining SSL Certificates on WebLogic.

WebSphere

Follow the instructions found in *Enterprise PeopleTools PeopleBook: System and Server Administration,* "Working with IBM WebSphere," Setting Up SSL on WebSphere.

If an HTTP server is also deployed, follow the instructions in *Enterprise PeopleTools PeopleBook: System and Server Administration,* "Working with IBM WebSphere," Setting Up SSL on IBM HTTP Server.

How to Disable HTTP on a Web Server

You can do this at multiple levels. Start by configuring the web profile:

1. In PIA, navigate to PeopleTools, Web Profile, Web Profile Configuration.
2. Select the web profile that you want to configure; for example, PROD.
3. Select the Security page.
4. Select Secured Access Only.
5. Save your changes.

WebLogic

To further disable HTTP on a WebLogic server, first ensure that HTTPS is set up and working properly using the instructions in the previous section. Then do the following:

1. Log on to the WebLogic console.
2. Expand from the left panel PeopleSoft, Server, PIA.
3. On the right panel, select Configuration, General tab.
4. Deselect the Listen Port Enabled check box.
5. Select Apply.

WebSphere

To further disable HTTP on the WebSphere server, first ensure that HTTPS is set up and working properly using the instructions in the previous section.

In WebSphere, you can disable HTTP by converting an HTTP port into an HTTPS port, as follows:

1. Expand Servers, Application Server, *server_name*, Web Container, HTTP Transport.
2. Click the relevant HTTP port.
3. Select the Enable SSL check box.

4. Select the SSL drop-down that is tied to the certificates.
5. Save the configuration and log off.
6. Restart the WebSphere server.

How to Change the Default Password of PSKEY

PSKEY is a keystore file located in the *PS_HOME*\webserv*domain*\keystore directory. The file contains all root and node certificates used by the Integration Gateway and PIA. The keystore file is shipped with a default password of *password*, which should be changed. Use a combination of uppercase and lowercase letters and numbers in the password.

To change the default password:

1. Use pskeymanager.bat (pskeymanager.sh on UNIX) to change the default password. Enter the following at a command prompt:

   % pskeymanager -changeKeystorePassword
2. Enter the old password, then the new password, for example, *Sec123Pass*.
3. Update the `secureFileKeystorePasswd` property in the integration.properties file with the *Sec123Pass* string.

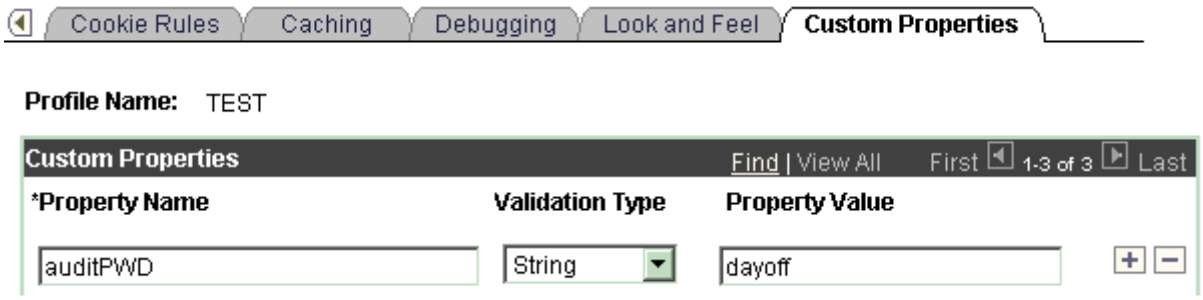
   Note that unlike other passwords in this file, the secureFileKeystorePasswd is not encrypted.
4. Because the web server (WebLogic or WebSphere) also uses this keystore, you must update the password for the web server as well with the string *Sec123Pass*.

   See the previous section "How to Enable SSL on a Web Server for HTTPS."

How to Disable Configuration Re-Initialization

The configuration that enables dynamic re-initialization is only set by default on the PROD web profile; no other profile has this setting enabled. However, an administrator may possibly have set this on a production system. To ensure that this setting is off, follow these steps:

1. In PIA, navigate to PeopleTools, Web Profile, Web Profile Configuration.
2. Select the web profile that you want to configure, for example, PROD.
3. Select the Custom Properties page.
4. Delete any property with the name auditPWD, as in the following example:



5. Save your changes.

How to Disable Browser Caching

A browser will cache various pages and states in memory to increase performance. You may need to disable these performance features on the browser for security reasons. Note that once caching is disabled, the Back button on the browser stops working in PIA.

To disable caching:

1. In PIA, navigate to PeopleTools, Web Profile, Web Profile Configuration.
2. Select the web profile that you want to configure, for example, PROD.
3. Select the Caching page.
4. Make sure that the Cache Generated HTML and Cache Homepage check boxes are both deselected.
5. Save your changes.

How to Configure a Forward Proxy Server for the Portal and Integration Gateway

To configure a forward proxy server for the Portal and the Integration Gateway, set the following system properties:

```
http.proxyHost=proxy.corp.com
http.proxyPort=5080
https.proxyHost=proxy.corp.com
https.proxyPort=5443
```

Where *proxy.corp.com* is the machine running the proxy server, and 5080 and 5443 are examples of the HTTP and HTTPS listening ports for the proxy, respectively. These system values are set differently for WebLogic and WebSphere and are shown in the following sections.

Setting a Forward Proxy Server for WebLogic

For WebLogic, edit the setEnv.cmd (setEnv.sh on UNIX) and set the following environment variables:

```
# HTTP_PROXY_ENABLE       - Enable the use of the following forward http proxy
# HTTP_PROXY_HTTPHOST     - IP/hostname of forward http proxy server to for HTTP requests.
#
# HTTP_PROXY_HTTPPORT     - HTTP Port number of forward http proxy server.
# HTTP_PROXY_HTTPSHOST    - IP/hostname of forward http proxy server for HTTPS requests
#
# HTTP_PROXY_HTTPSPORT    - HTTPS Port number of forward http proxy server.
```

Setting a Forward Proxy Server for WebSphere

Set the properties using the WebSphere Administration console:

1. Log on to WebSphere Administration console.
2. Expand Servers, Application Servers, server1, Process Definition, Java Virtual Machine, Custom Properties.
3. Click New Key/Value pair and add the following new pairs:

   Key="http.proxyHost", Value="*forward proxy hostname*"
   Key="http.proxyPort", Value="*forward proxy HTTP port*"
   Key="https.proxyHost", Value="*forward proxy hostname*"
   Key="https.proxyPort", Value="*forward proxy HTTPS port*"
4. Save the configuration changes, log off, and restart WebSphere.

How to Bypass a Forward Proxy for Local Hosts

To bypass a forward proxy server for Portal and Integration Gateway, set up the following system property:

```
http.nonProxyHosts=machinename1.corp.com|machinename2.corp.com|...
```

Use a different machine name for each host that you want to bypass. The value is a list of host names separated by the pipe (|) symbol. For example, to bypass the proxy for hosts *a.corp.com* and *b.corp.com*, the value should be:

```
http.nonProxyHosts=a.corp.com|b.corp.com
```

You can also bypass all servers in a domain by using an asterisk (*) as a wildcard, indicating that all servers in .corp.com domain are bypassed from using the proxy.:

```
http.nonProxyHosts=*.corp.com
```

You set this property (one value) for both HTTP and HTTPS. The system value is set differently for WebLogic and WebSphere, as discussed in the following sections.

How to Bypass Forward Proxy for Local Hosts for WebLogic

For WebLogic, edit setEnv.cmd (setEnv.sh on UNIX) and set the corresponding environment variables:

```
# HTTP_PROXY_NONPROXY_HTTPHOSTS  - Host names and domain names of HTTP content
#                                  to not proxy.
```

How to Bypass Forward Proxy for Local Hosts for WebSphere

Set the property using the WebSphere Administration console.

1. Log on to the WebSphere Administration console.
2. Expand Servers, Application Servers, server1, Process Definition, Java Virtual Machine, Custom Properties.
3. Click New Key,Value pair and add the following new pairs:

   ```
   Key="http.nonProxyHosts"
   Value="machinename1.corp.com|machinename2.corp.com|..."
   ```
4. Save the configuration changes, log off and restart WebSphere.

How to Enable Mutual Authentication for Integration

Common practice is to use certificate-based mutual authentication for the Integration Gateway. To set up your Integration Gateway for mutual authentication, please follow the instructions in *Enterprise PeopleTools PeopleBook: PeopleSoft Integration Broker,* "Setting Up Secure Messaging Environments."

How to Enable LDAPS for Directory Integration

LDAP directory access should be configured to be secure by using LDAP over SSL (LDAPS). The process is described in *Enterprise PeopleTools PeopleBook: Security Administration*, "Employing LDAP Directory Services," Using LDAP Over SSL.

How to Enable TUXEDO Encryption

To enable TUDEDO-level encryption, edit the configuration file psappsrv.cfg for the domain. Change the Encryption property for the Workstation Listener and the JOLT Listener sections. The default value of 0 does not encrypt. Change the value to 64 for 64-bit encryption or to 128 for 128-bit encryption:

```
[Workstation Listener]
;===========================================================================
; Settings for Workstation Listener
;===========================================================================
;Address Note: Can be either Machine Name or IP address.
;Address Note: %PS_MACH% will be replaced with THIS machine's name
Address=%PS_MACH%
Port=7000
```

```
Encryption=128
Min Handlers=1
Max Handlers=2
Max Clients per Handler=40
Client Cleanup Timeout=60
Init Timeout=5
Tuxedo Compression Threshold=5000

[JOLT Listener]
;=============================================================================
; Settings for JOLT Listener
;=============================================================================
;Address Note: Can be either Machine Name or IP address.
;Address Note: %PS_MACH% will be replaced with THIS machine's name
;Address Note: 0.0.0.0 enables JSL to bind to all IP addresses mapped for this machine
Address=0.0.0.0
Port=9000
Encryption=128
Min Handlers=1
Max Handlers=2
Max Clients per Handler=40
Client Cleanup Timeout=60
Init Timeout=5
Client Connection Mode=ANY
Jolt Compression Threshold=1000000
```

USEFUL HARDENING LOCKDOWN LINKS

Securing the WebLogic Server Host

http://download.oracle.com/docs/cd/E14571_01/wls.htm

Scroll down to:
Security > Securing a Production Environment
> Ensuring the Security of Your Production Environment
> Securing the WebLogic Server Host

"A WebLogic Server production environment is only as secure as the security of the machine on which it is running. It is important that you secure the physical machine, the operating system, and all other software that is installed on the host machine."

PeopleSoft Enterprise supports Oracle 9i (and later) Advanced Security Option My Oracle Support (logon required)

https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=763255.1

"... PeopleSoft is pleased to announce that PeopleSoft Enterprise now supports Oracle 9i Advanced Security Option (ASO). We have had numerous requests from customers for this support and have recently completed the testing necessary for us to certify the use of ASO with Enterprise applications. Customers interested in using ASO can do so with any version of PeopleTools that supports Oracle 9i (PT 8.1x, PT 8.2x, and PT 8.4x)."

Oracle Database Security Checklist

http://www.oracle.com/technology/deploy/security/database-security/pdf/twp_security_checklist_database.pdf

Project Lockdown is a phased approach to securing your database infrastructure:

http://www.oracle.com/technology/pub/articles/project_lockdown/project-lockdown.pdf.

Chapter 5 - PeopleTools Security Hardening

PeopleSoft applications are depended on to deliver data in a secure, reliable fashion. Data integrity, confidentiality, and availability must be maintained. PeopleTools must be installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

This chapter describes the requirements for installing and operating PeopleTools in a secure fashion to maintain the security integrity of PeopleTools and the application software. This chapter applies to all individuals who are responsible for installation of new software, operation of existing software, and security administration.

Before a PeopleSoft application is put into production, you should take reasonable steps to ensure that PeopleTools security has been hardened. Through the appropriate use of PeopleTools authentication, authorization, and audit functionality, you can help mitigate risk to your security infrastructure.

The hardening procedure is a group of tasks that should be completed to harden PeopleTools. Many of these items are industry-standard best practices; others are specific to PeopleTools. This list is by no means exhaustive; however, it should give you a feel for items to check. Some of the general steps included in the PeopleTools hardening procedure include:

- Deleting or disabling unused user IDs.
- Setting security parameters.
- Enabling audit logging.
- Appling security patches to keep software properly updated.

Delete or Disable Unused User IDs

Every delivered PeopleSoft database comes with several default User IDs. Before migrating a database into production, it is critical that you identify these IDs and either delete or disable them.

To delete a user profile:

1. Select PeopleTools, Security, User Profiles, Delete User Profiles to access the Delete User Profile page.
2. Make sure that you have selected the *correct* user profile.
3. Click Delete User Profile to remove information related to this particular user profile that appears in PeopleTools, application tables, and every security table in the system.

To disable a user profile:

1. Select PeopleTools, Security, User Profiles, User Profiles to access the Find Existing Values page.
2. Select the user ID that you want to disable.
3. Select the Account Locked Out check box to disable the user profile. The user can't sign on until you deselect this check box again.

Enable Password Controls

If you're using PeopleSoft user ID and password authentication, you are strongly encouraged to enable password controls and follow industry best practices with regard to the settings. You use the Password Controls page to set password restrictions such as duration and minimum length of a password that you might want to impose on your end users.

Select PeopleTools, Security, Password Configuration, Password Controls to access the Password Controls page.

Here are the available options:

Enable Signon PeopleCode Select this check box to enable the Age and Account Lockout password controls. The other password controls are not enabled by this field.

If you don't want these password controls when, for example, you already have a third-party

utility that performs equivalent features, leave this check box deselected.

Note. You can extend or customize the controls by modifying the PeopleCode.

Age

You define a number of days (between 1 and 365) that a password is valid. To do this, select the Password Expires in *N* Days option. Users signing on after a password expires must change their passwords before they can sign on. If you don't want the password to expire, select *Password Never Expires*. When a password expires, the user can't sign on to the system and will be prompted to change it.

If you want to specify a period during which the system warns users that their password is about to expire, you have the following options:

- If you want to specify a warning period, select Warn for *N* Days, and enter the number of days in the edit box.
- If you don't want any warning period, select *Do not warn of expiration*.

PeopleSoft delivers a default permission list named PSWDEXPR (Password Expired). When a password expires for a user, the system automatically revokes all of that user's roles and permission lists and temporarily assigns them the PSWDEXPR permission list only.

A user whose password has expired can access only items in the PSWDEXPR permission list, which typically grants access to the Change Password component only. For the duration of the session, until the user changes the password, the user is restricted solely to the PSWDEXPR permission list.

Note. The actual user profile stored in the database is not changed in any way when the password expires. You don't need to redefine the profile. When the password is changed, the system restores the user profile's previous roles and permission lists.

Account Lockout

This control enables you to lock an account after a specified number of failed logon attempts. For example, if you set the Maximum Logon Attempts value to *3*, and a user fails three consecutive logons, he or she is automatically locked out of the system. Even if the user correctly enters a user ID and password on the fourth attempt, the user is not permitted to log on on. This feature reduces the risk of any "brute force" intruders into your system. It also provides a reminder to your end users to remember the password they choose.

After the account is locked out, a system administrator needs to open the user profile and deselect the Account Locked check box manually.

Miscellaneous

The Allow password to match User ID control enables administrators to ensure that users don't use their own user ID as a password. This helps you prevent hackers from guessing passwords based on a list of employee names.

Minimum Length

Administrators can opt to set a minimum length for passwords maintained by the PeopleSoft system. If the minimum length is set to *0*, the PeopleSoft password controls do not enforce a minimum length on the user's password. This does not, however, imply that the password can be blank. When you create a new user or a user changes a password, the system checks this value. If it is not zero, the system tests the password to ensure that it meets length requirements, and if it doesn't, an error message appears.

Character Requirements

Administrators can require a set number of digits or special characters within a password. Special characters, or *specials*, are symbols such as # and @, and digits are numbers (integers), such as 1 or 2.

Here is the list of special characters that you can include within a password:

```
! @ # $ % ^ & * ( ) - _ = + \ |[ ] {} ; : / ? . > <
```

Purge User Profiles

This setting enables you to purge the system of user profiles that have not been used in a specified amount of time. This aids in general housekeeping. In particular, if you maintain user profiles in a directory server, a row is still added to the PSOPRDEFN table for the system to access while the user interacts with the system. However, if that user is deleted from the directory server, you still need to delete the row in PSOPRDEFN that is associated with the deleted user profile.

Note. The Application Engine program that performs this operation is named PURGEOLDUSERS.

Expire Password At Next Logon

If you're using PeopleSoft password controls, we recommend that you use this option to force users to change their passwords in the following situations:

- The first time that a user signs in to PeopleSoft.
- The next time that a user signs in.
- The first time that a user signs in after the system has emailed the user a randomly generated password.

To set this option:

1. Select PeopleTools, Security, User Profiles, User Profiles to access the Find Existing Values page.
2. Select the user ID that you want.
3. On the General page, select the Expire Password At Next Login check box.

Note. To use this option, you must first enable the Password Expires in *N* Days PeopleSoft password control

Allow Password to be Emailed

PeopleTools contains functionality that will enable users to receive a new password via email if they have forgotten their existing one. At some sites, the security administrator may not want passwords appearing unencrypted in anyone's email. You implement this feature using a permission list. None can use it, some can use it, or all can use it, depending on your implementation. Users who don't have the proper authority receive an error message if they attempt to have a new password emailed to them.

To change this setting:

1. Select PeopleTools, Security, Permissions & Roles, Permission Lists.
2. On the search page, search for the permission list that you want to modify and select it.

   The Permission List component appears.
3. On the General page, review the setting of the Allow Password to be Emailed check box.

Note. If the user is a member of at least one permission list for which this check box is selected, then they will be allowed to have a new password emailed.

Review Sign-in and Time-out Security

A user attempting to sign in to PeopleSoft enters a user ID and a password on the PeopleSoft Signon page. If the ID and password are valid, PeopleSoft connects the user to the application, and the system retrieves the appropriate user profile.

If the user attempts to sign in during an invalid sign-in time, as defined in the user's security profile, the user is not allowed to sign in. A sign-in time is an adjustable interval during which a user is allowed to sign in to PeopleSoft. For example, if a given sign-in time is Monday through Friday from 7 a.m. to 6 p.m. for a set of users, those users cannot access a PeopleSoft application at any time on Saturday or on Friday at 6:05 p.m.

After a user signs in, he or she can stay connected as long as the sign-in time allows and as long as the browser doesn't sit idle for longer than the time-out interval. A time-out interval specifies how long the user's machine can remain idle before PeopleSoft automatically disconnects the user from the application.

You specify both the sign-in times and the time-out interval using PeopleTools Security. The sign-in times are maintained on the Signon Times page of the permission list. The time-out settings are maintained on the General page of the permission list. These settings should be reviewed prior to moving a PeopleSoft application into production.

CHANGE THE ACCESS PASSWORD

The PeopleSoft access ID is the RDBMS ID with which PeopleSoft applications are ultimately connected to your database after the PeopleSoft system authenticates the user. The access ID has all the RDBMS privileges necessary to access and manipulate data for an entire PeopleSoft application.

Due to the privileges associated with the access ID, it is extremely important that you choose a strong access password (for example, minimum length of 8 characters, including any combination of mixed case, numerals, and special characters, and so on.). Generally, we recommend that only your database administrator should know this password. In addition, we recommend that this password be changed periodically (for example, every 30 days).

To change an Access Profile password

1. In Application Designer, select Tools, Miscellaneous Definitions, Access Profiles.

   The Access Profiles dialog box appears.

2. In the Access Profiles list, highlight the profile that you want to modify and click Edit.

   The Change Access Profile dialog box appears. This dialog box provides fields to enter the old password and the new password, and to confirm the new password for the Access Profile.

3. Enter and confirm the new password.

   The Access Password is the password string for the ID. Confirm Password is a required field and its value must match that of Access Password.

4. Click OK.

CHANGE THE CONNECT PASSWORD

The connect ID is an RDBMS ID that's used to perform the initial connection to the database when an application server is booted, or during a two-tier connection. Although this ID only has select privileges on a handful of tables, we still recommend that you select a strong connect password, keep it confidential, and change it periodically.

To change the connect password, you'll need to follow your RDBMS-specific instructions. After you've changed the password, remember that you'll also need to change it in your application server configuration and in Configuration. When specifying the connect password for an application server in the PSADMIN utility, be sure to select the option to encrypt it.

If you have two-tier users, we recommend that you set the connect password once in Configuration Manager and then roll the configuration out to your user community.

CHANGE THE IB GATEWAY PROPERTIES PASSWORD

The default username and password combination for accessing the Integration Broker gateway properties is *administrator*/*password*. This password should be changed prior to production.

On the authentication page that protects gateway properties administration, a check box is available labeled Change password. Selecting this check box when signing in enables an administrator to change the default password to a password that follows stricter (for instance corporate policy) password guidelines.

REVIEW THE SINGLE SIGNON CONFIGURATION

PeopleSoft supports single signon within PeopleSoft applications. Within the context of your PeopleSoft system, single signon means that after a user has been authenticated by one PeopleSoft application server, that user can access a second PeopleSoft application server without entering an ID or a password. Although the user is actually accessing different applications and databases, the user navigates seamlessly through the system. Recall that each suite of PeopleSoft applications, such as HR or CRM, resides in its own database.

After the first application server and node authenticates a user, PeopleSoft delivers a web browser cookie containing an authentication token. PeopleSoft Internet Architecture uses web browser cookies to store a unique access token for each user after he or she are authenticated initially. When the user connects to another PeopleSoft application server and node, the second

application server uses the token in the browser cookie to re-authenticate the user behind the scenes so that they don't have to complete the sign-on process again.

Single signon is critical for PeopleSoft portal implementations because the portal integrates content from various data sources and application servers and presents them in a unified interface. When users sign in through the portal, they always take advantage of single signon. Users need to sign on once and be able to navigate freely without encountering numerous signon screens.

Before a PeopleSoft application is migrated into production, reviewing the single signon configuration is very important. For each database, you should review which nodes you're going to accept authentication tokens from. You do not want a production system accepting authentication tokens from an untrusted system (or a system it should not trust). To review your single signon configuration, select PeopleTools, Security, Security Objects, Single Signon to access the Single Signon page

Here is a brief description of the items on this page:

Expiration time in minutes You need to set an expiration time for the tokens that this system accepts for authentication.

Message Node name Shows the name of a trusted message node. To share authentication tokens between nodes, the nodes need to trust each other. By adding a node to this grid, you indicate that a particular node is known to the system and trusted. When a node is trusted, the local node accepts tokens issued by it.

Local Node Indicates whether the node is local.

See also *Enterprise PeopleTools PeopleBook: Security Administration,* "Setting up Digital Certificates and Single Signon."

USE STRONG NODE PASSWORDS OR USE CERTIFICATES

When you configure nodes for single signon, two authentication options are available: Password and Certificate. The more secure of these two is Certificate. If you choose to use Password, be sure to select a strong password and change it periodically.

You set up node definitions using the Portal, Node Definitions component. The two options related to single signon are as follows:

Authentication Option Determines how nodes in a single signon configuration authenticate other nodes in the same configuration. You have the following options:

None. Specifies no authentication between nodes.

Note. This option conflicts with PeopleSoft Integration Broker. If you select None, PeopleSoft Integration Broker messaging will fail, as will Single Signon.

Password. Indicates that each node in the single signon configuration authenticates other nodes by way of knowing the password for each node. For example, if three nodes exist (A, B, and C), the password for node A needs to be specified in its node definition on node A, B, and C.

Certificate. Indicates that a digital certificate authenticates each node in the single signon configuration. PeopleSoft recommends using certificate authentication for single signon. For certificate authentication, you need to have the following in the key store in the database for each node:

- A digital certificate for each node.
- The root certificate for the CA that issued the node certificate.

Important! For single signon, the alias for the certificate of a node needs to be the *same* as the node name. You *must* set up your digital certificates before you select *Certificate* as the authentication option.

Default Local Node The default local node is used specifically for setting up single signon. This indicates that the current node represents the database you're signed in to. The options that you set for single signon should be made in the default local node definition.

REVIEW SIGNON PEOPLECODE AND USER EXITS

Signon PeopleCode is delivered that allows you to enable directory-based authentication, password controls, and other functionality. In addition, signon PeopleCode and user exits can be used to customize the authentication process.

Before putting a system into production, all signon PeopleCode and user exits should be carefully reviewed and tested. Mistakes in this area could lead to serious authentication vulnerabilities.

Please refer to *Enterprise PeopleTools PeopleBook: Security Administration,* "Employing Signon PeopleCode and User Exits" for detailed information about this topic.

LIMIT USAGE OF THE PEOPLESOFT ADMINISTRATOR ROLE

Generally, only a handful of users—perhaps even just one user—should have the PeopleSoft Administrator role. A user with this special role is authorized for virtually everything within the PeopleSoft system. Keeping at least one user ID with this role is essential so that you will not be in a situation in which you're locked out of the security administration pages. You should choose a strong password for this user and change the password periodically.

The Roles component includes queries that you can run to determine which users are associated with each role.

LIMIT ACCESS TO APPLICATION DESIGNER AND DATA MOVER

In a development system, numerous users will likely have access to PeopleSoft Application Designer and PeopleSoft Data Mover; however, in a production system, access to these development tools should be strictly limited.

Generally, these development tools should not be used in production. Rather, development should be done in a separate database, tested, and then migrated into production using the upgrade tools.

Note that if any users can access development tools in a production system, they can change virtually any data in the database. For example, with PeopleSoft Data Mover access or a SQLExec in PeopleCode, any SQL could be run against the database.

To lock down access to the design tools, review the settings on the PeopleTools page of the Permission List definition.

LIMIT ACCESS TO USER PROFILES, ROLES, AND PERMISSION LISTS

In your production system, only your security administrator should have access to the user profiles, roles, and permission lists. If any other users have access to these components, they could possibly elevate their own privilege levels.

Several queries are delivered for user profiles, roles, and permission lists that will provide a good picture of who has access to what. This information should be carefully reviewed prior to going live as well as periodically to ensure that security policies and guidelines are being maintained.

LIMIT ABILITY TO START APPLICATION SERVER

On the General page of the Permission List component is a check box titled Can Start Application Server?. This option should be selected only for the user ID that's being used to start the application server; otherwise, a rogue application server could possibly be started.

Can Start Application Server?

Select to enable a user profile with this permission to start a PeopleSoft application server. This can be a user ID used solely for starting the application server. At least one of the permission lists associated with the user ID used for starting the application server must have this permission selected.

This user ID is not the user ID of the actual user who signs in to an application server and starts it by submitting the appropriate commands. Rather, this option applies to the user ID and password that you enter into PSADMIN (or PSAPPSRV.CFG) in the Startup section. This is the user ID that the application server uses to connect to the database. In many installations, the application server starts with an automated process, not by a user physically submitting the commands.

When you build an application server domain, one of the parameters that an administrator enters is a PeopleSoft user ID (and password). These values are contained in a configuration file that BEA Tuxedo reads when the application server is started. The user ID stored in the file is the user ID that requires the Can Start Application Server option set in a permission list with which it's associated.

Note. This permission also applies to starting a PeopleSoft Process Scheduler server. Password controls don't apply for the user profile that's used to start the application server.

REVIEW QUERY SECURITY

PeopleSoft Query is an end user-reporting tool that helps you build SQL queries to retrieve information from your application tables.

Query takes advantage of a user's security settings, row-level security, and primary permission list. You can specify the records that each Query Manager or Query Viewer user is allowed to access when building and running queries.

Note that Query permissions are enforced only when you are using Query; it doesn't control runtime page access to table data.

Permission Lists

Use Query Access Manager (PeopleTools, Security, Query Security, Query Access Manager) to define query access group trees. Each tree contains access groups (nodes) and records (PeopleSoft record definitions) categorized by function (similar to folders in Microsoft Windows).

After you build a query access group tree, you give users access to one or more of its access groups using the Permission List Access Groups page (PeopleTools, Security, Permissions and Roles, Permission Lists and click the Query tab, Access Permissions link).

Row-Level Security

With row-level security, users can access a table (record) without having access to all rows on that table. PeopleSoft applications implement row-level security by using a SQL view that joins the data table with an authorization table. When a user searches for data in the data table, the system performs a related record join between the view and the base table rather than searching the table directly. The view adds a security check to the search, based on the criteria you've set up for row-level security.

Row-level security is implemented in the Application Designer. Open the desired record definition, click the Properties button, and select the Use tab from the Record Properties dialog box. Then select the security record definition (usually a view) in the Query Security Record list box.

Query is a very powerful tool and thus query security should be reviewed very carefully prior to production.
Please refer to *Enterprise PeopleTools PeopleBook: Security Administration*, carefully prior to production. Properties button, and

ENABLE SQL ERROR MESSAGE SUPPRESSION

You can enable SQL error suppression by updating the PeopleSoft application server configuration file. This file, called psappsrv.cfg, can be found in the application server directory under the database-named folder. Add the following line to the file:

```
Suppress SQL Error = 1
```

Generally, you'll want detailed SQL errors during development; however, in a production environment, best practice is to suppress the SQL error messages. If attackers can manipulate SQL queries through parameters, input fields, or in specialized locations such as Query Manager, they can generate invalid SQL that causes the database to return an error message to the application server. When the application displays this error message, the attackers gain information about the underlying query structure, database type, table names, column names, and other useful information that could be used to launch more sophisticated attacks. Database attack is much more difficult when attackers must guess blindly at query structure and cannot view error messages to understand why specially constructed queries fail.

TRACK USERS' LOGIN AND LOGOUT ACTIVITY

PeopleSoft Security provides two audit logs that track users' sign-in and sign-out activity in PeopleSoft. Sign-out activity includes time-outs, browser closings, and browser freezes.

See: http://download.oracle.com/docs/cd/E15645_01/pt850pbr0/eng/psbooks/tsec/book.htm

Access these logs by navigating to PeopleTools, Security, Common Queries. Select Access Log Queries, then one of the following logs:

- Access Activity by User

  View a single user's login and logout activity. This log includes a user's Client IP address, login times and logout times.

- Access Activity by Day

  View one or more days of all user logins and logouts. This log includes user IDs, client IP addresses, and login times and logout times.

DECOUPLING PS_HOME AND PS_CFG_HOME

Understanding PS_HOME and PS_CFG_HOME

http://download.oracle.com/docs/cd/E15645_01/pt850pbr0/eng/psbooks/tsvt/book.htm?File=tsvt/htm/tsvt04.htm#H3002

On any server that you install the PeopleSoft software, the installation program installs the required files for that server into one high-level directory structure, referred to as PS_HOME. After the program creates a domain, the configuration files associated with that domain reside in a directory structure referred to as PS_CFG_HOME.

By default, the system separates the binary files (executables and libraries) stored in PS_HOME from the ASCII files (configuration and log files) associated with a domain stored in PS_CFG_HOME. This separation of the binary and ASCII files applies only to these servers:

- PeopleSoft Application Server.
- PeopleSoft Process Scheduler Server.
- PeopleSoft Search Server.

The decoupling of the file types in these separate directory structures enables system administrators to:

- Streamline and provide more flexible PeopleSoft server installations.
- Apply unique security restrictions to the binary file and configuration file locations.

New Directories

PS_HOME

- Compiled, non-modifiable executables and libraries.

PS_CFG_HOME

- Text files associated with the configuration and administration of a domain that can be viewed, modified, or generated by the system.

Securing PS_HOME and PS_CFG_HOME

http://download.oracle.com/docs/cd/E15645_01/pt850pbr0/eng/psbooks/tsvt/book.htm?File=tsvt/htm/tsvt15.htm#H2001

With the separation of the PS_HOME and PS_CFG_HOME directories, system administrators can implement more secure PeopleSoft deployments by restricting access within each of these directory structures.

This section describes the procedures and considerations involved in configuring these additional security options.

- Understanding PS_HOME Security
- Understanding PS_CFG_HOME Security
- Configuring Partial PS_HOME Access
- Multiple Administrator User Accounts
- Implementing PS_CFG_HOME Security

CONSIDER AUDITING

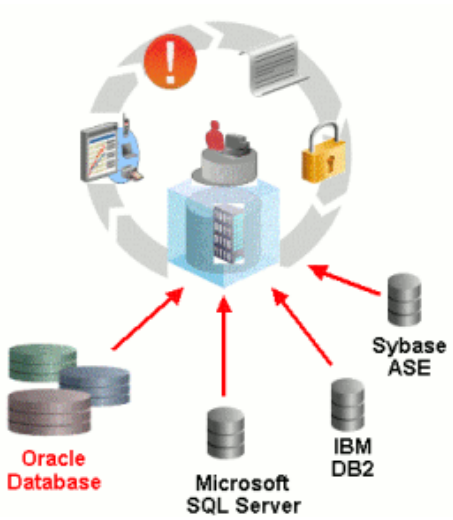
Part of any successful security strategy is auditing. PeopleTools provides two methods of auditing, which you should review and consider using in your production system. For more information about the two alternatives, please see the following documentation:

See *Enterprise PeopleTools PeopleBook: Data Management,* "Employing Database Level Auditing."

See *Enterprise PeopleTools PeopleBook: PeopleSoft Application Designer,* "Creating Record Definitions," Creating User-Defined Audit Record Definitions.

Oracle Audit Vault

Satisfying compliance regulations such as SOX, PCI, and HIPAA and mitigating security risks are among the top security challenges businesses face today. Today the use of audit data as a security resource remains very much a manual process, requiring IT security and audit personnel to sift through large amounts of dispersed audit data and create reports to meet internal and external auditor requirements.



Oracle Audit Vault automates the audit collection, monitoring and reporting process, turning audit data into a key security resource for detecting unauthorized activity. The latest release of Oracle Audit Vault 10.2.3.2 now supports monitoring Microsoft SQL Server 2000, 2005, and 2008, IBM DB2 UDB 8.2 through 9.5, and Sybase ASE 12.5.4 through 15.0.x databases. This new capability enables customers to use a single monitoring solution for the following databases:

- Oracle
- Microsoft SQL Server
- IBM DB2 UDB
- Sybase ASE

The Oracle Audit Vault Reports interface provides entitlement reports with up-to-date snapshots of Oracle Database users, privileges, and profiles, which enable auditors to track changes to database access and out-of-the-box reports to help meet compliance regulations as well as charting capabilities.

Chapter 6 - Securing Customized PeopleSoft Applications

PeopleSoft devotes a lot of attention and resources to delivering a secure product to its customers. However, most customers don't implement PeopleSoft applications as they are delivered. To enable customers to meet their unique business needs, PeopleSoft software can be configured in many ways. If your organization modifies the delivered applications, this new code must be secured.

If you modify the delivered PeopleSoft application, use the following guidelines to verify that these changes don't compromise the security of your implementation:

- Every component should have appropriate row-level security.
- Defend against SQL injection. All user-entered data that is part of dynamic SQL must be isolated to a bind variable.
- All user-entered HTML must be escaped.
- All hidden page fields should have the Modifiable by HTML flag deselected with the exception of those that are used to control the user interface.
- All user-entered file names should not contain complete or relative paths.

Configure Every Component for Row-Level Security

Every component should apply row-level security that's appropriate for the end user.

Note. In some cases, NONE (or no row-level security) is appropriate.

Row-level security can be implemented in several ways, such as:

- Applying security using search views.
- Applying security using search prompt views.
- Applying security using an application-specific framework. (For example, HR manager self-service or application-coded search pages.)

Determine the method used by your product or product line and ensure that your component adheres to the standards used for that product.

Isolate All User-Entered Data to a Bind Variable

Take care anytime you construct a SQL statement using user input as part of that statement. Never allow the end-user to enter a string that contains an entire SQL statement or a SQL fragment. To ensure security, use the user data as a bind variable rather than concatenating it to a SQL statement.

For example, suppose that the user supplies a value for a WHERE condition:

Good: SELECT ABC FROM TABLE A WHERE A = :1

Bad: SELECT ABC FROM TABLE A WHERE A = | *user-entered-value*

Escape All User-Entered HTML

If you're writing your own HTML and plan to use user-supplied values, then user values should contain displayable data and not scripts. All string data must be escaped by calling the EscapeHTML PeopleCode function.

Example: &myHTML = &myHTML | EscapeHTML(*&user-supplied string*)

TURN OFF MODIFIABLE BY HTML FOR HIDDEN PAGE FIELDS

If your HTML contains JavaScript that accesses hidden fields on a page, ensure that the page field property Modifiable by HTML is enabled for the hidden field that you plan to modify.

The hidden field's logic should be limited to the user interface on the page. You should not code logic on the application server (that is, PeopleCode) that relies on data in hidden fields.

USER-ENTERED FILE NAMES SHOULD NOT INCLUDE PATHS

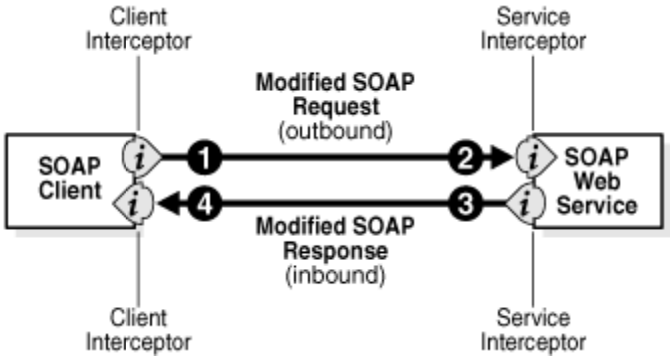
If you have applications that enable users to specify a destination path to store files, you should allow only file names and directories as separate items, instead of a path.

Good: Location: Appserver File: myfile.xxx (assuming that this is appended to a specified home location).

Bad: C:\appserver\myfile.xxx

WORKING WITH WEB SERVICE SECURITY (WS-SECURITY)

It is not practical to describe in detail here the full capabilities and implementation requirements for WS-Security with PeopleSoft. Please refer to PeopleBooks and the extensive documentation on oracle.com



See: http://download.oracle.com/docs/cd/B25221_04/web.1013/b15979/usecases.htm#CIHHHJIA

Understanding WS-Security

http://download.oracle.com/docs/cd/E15645_01/pt850pbr0/eng/psbooks/tsec/book.htm?File=tsec/htm/tsec12.htm#H3002

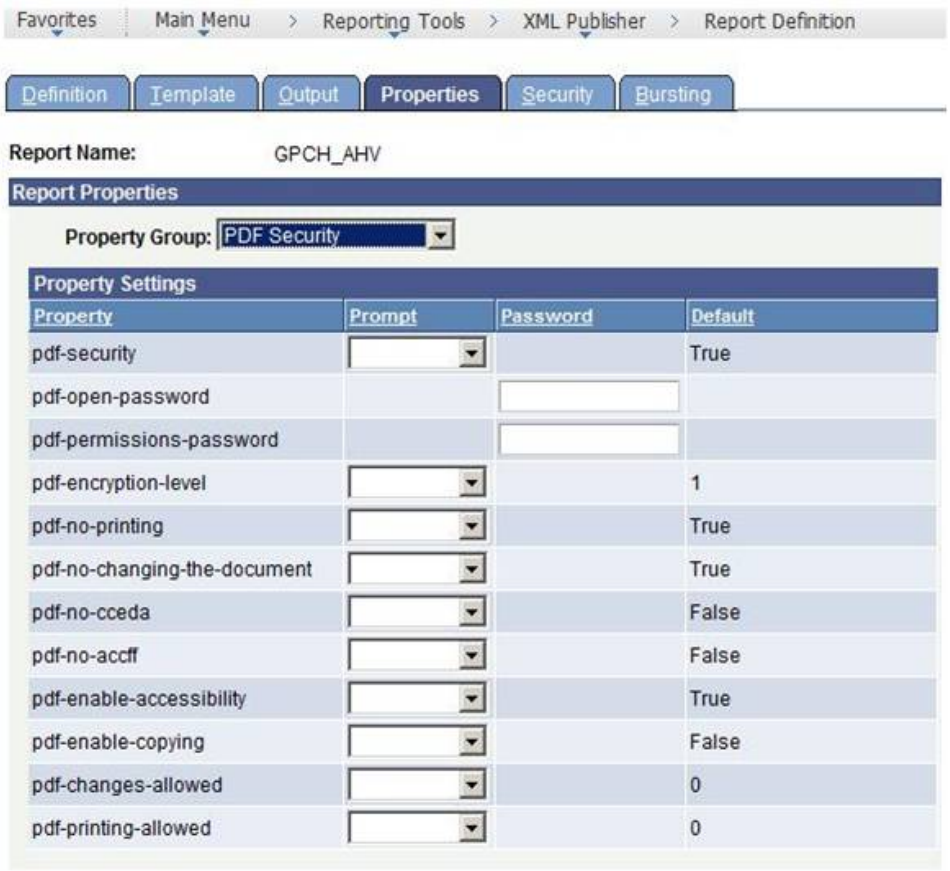
WS-Security provides a way to insert and convey security tokens in SOAP messages. The ability to leverage WS-Security standards provides for better interoperability and improved usability, enabling the implementation of robust security within a WSRP-capable environment.

The OASIS WS-Security specification is the open standard for web services security. Its goal is to let applications secure SOAP message exchanges by providing encryption, integrity, and authentication support. It provides authentication support for SOAP messaging. WS-Security offers these general-purpose mechanisms for associating security tokens with message content:

- Username token.
- SAML token.

PROTECTING PDF FILES AND XDO.CFG

In PeopleTools 8.50, the reporting development team incorporated this feature in the Report Definition page., See the following sample form.



To further enhance this capability, security-related properties can be overridden at runtime through PeopleCode the same as all other XMLP properties using the SetRuntimeProperties() method on the ReportDefn class. This is documented in PeopleBooks. Basically this method needs to be called right before the processReport() method is called:

Sample code snippet:

```
...
&asPropName = CreateArrayRept("", 0);
&asPropValue = CreateArrayRept("", 0);
&asPropName.Push("pdf-open-password");
&asPropValue.Push("test");
&oRptDefn.SetRuntimeProperties(&asPropName, &asPropValue);

&oRptDefn.ProcessReport(&sTemplateId, %Language_User, &dAsOfDate, &sOutputFormat);
```

Of course users should not hard-code the password value in the code; instead, if the password is stored encrypted in the database or somewhere else, they can use Decrypt() api

See the online PeopleBooks here for more information:
Hosted PeopleBooks http://www.oracle.com/pls/psft/homepage

You can read more about the configurable options in the Oracle Business Intelligence Publisher User's Guide here:
http://download.oracle.com/docs/cd/E10383_01/doc/bip.1013/b40017/T421739T421745.htm#4419522

Appendix A - Implementing Self Service or Gateway

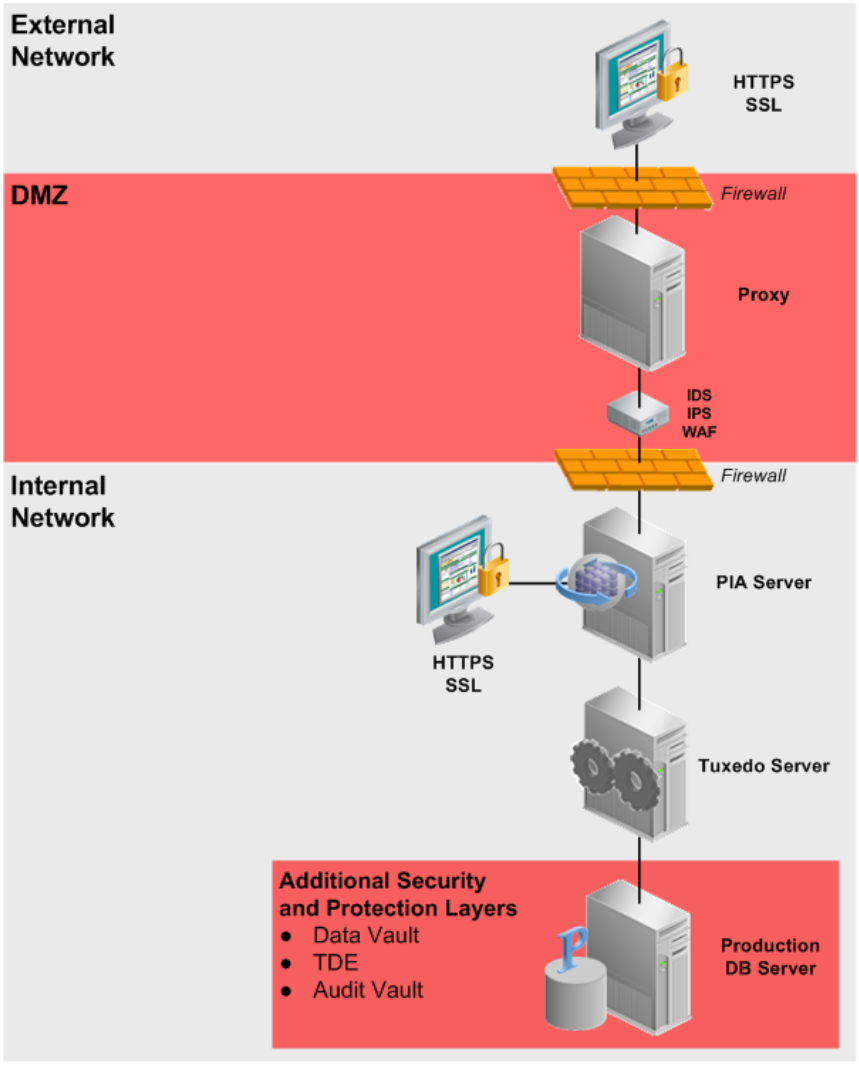
EXPOSING PEOPLESOFT OUTSIDE THE FIREWALL

This section presents a number of approaches to self-service architecture, based on discussions with customers and consultants. Extra layers of security are provided by Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Web Application Firewalls (WAF). None of these suggested deployments can be regarded as best because every customer environment is a compromise between the cost of the deployment and the evaluated risks. In these diagrams, the terms PIA Server and Tuxedo Server are used as logical rather than physical designations to differentiate the web server/Java application server and the business logic application server.

MANAGER AND EMPLOYEE SELF SERVICE

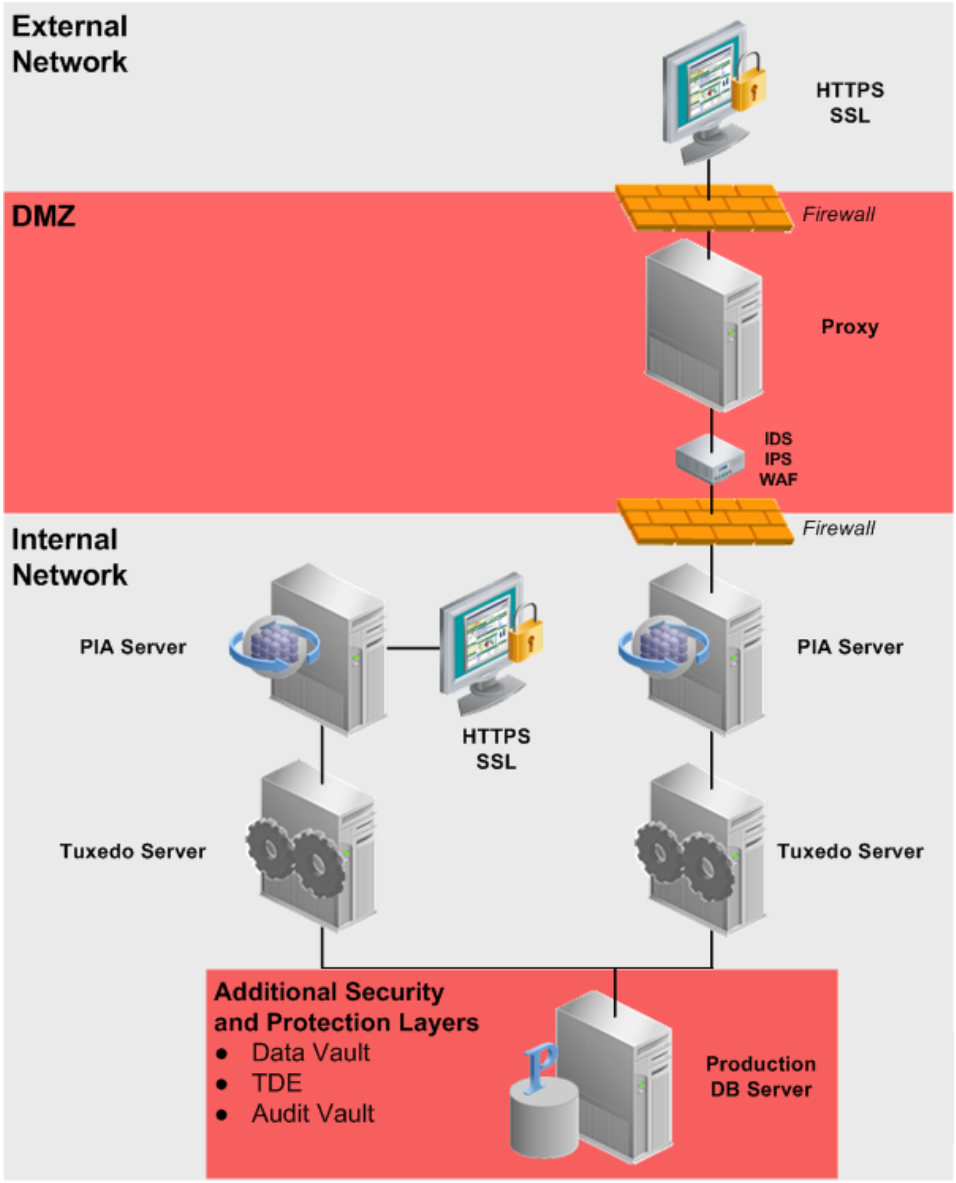
With Manager and Employee Self Service, a greater need exists for real-time and near real-time synchronization.

Example 1 is a single stack.



While the PeopleSoft instance is well-protected by the network protection devices, considering the additional database security products is worthwhile.

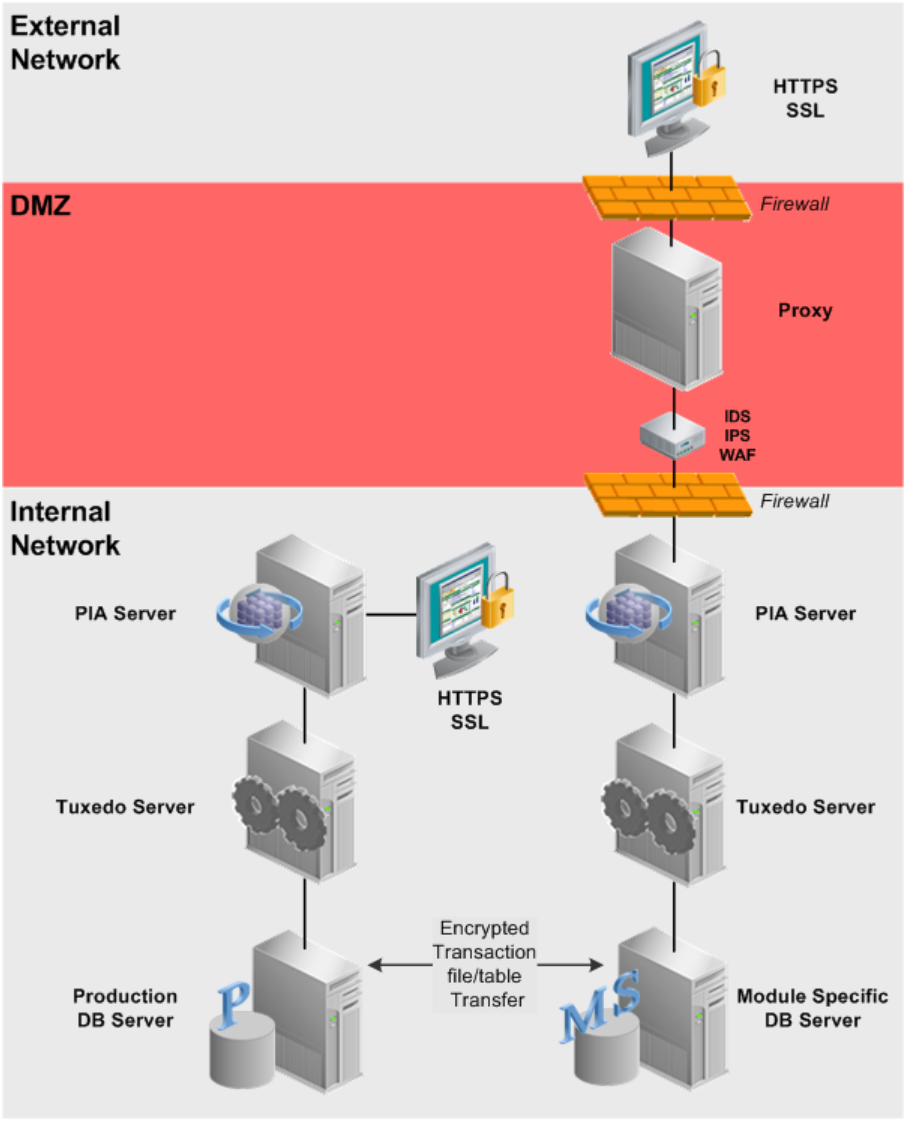
Example 2 is a dual stack with separate support for external access but using a common database.



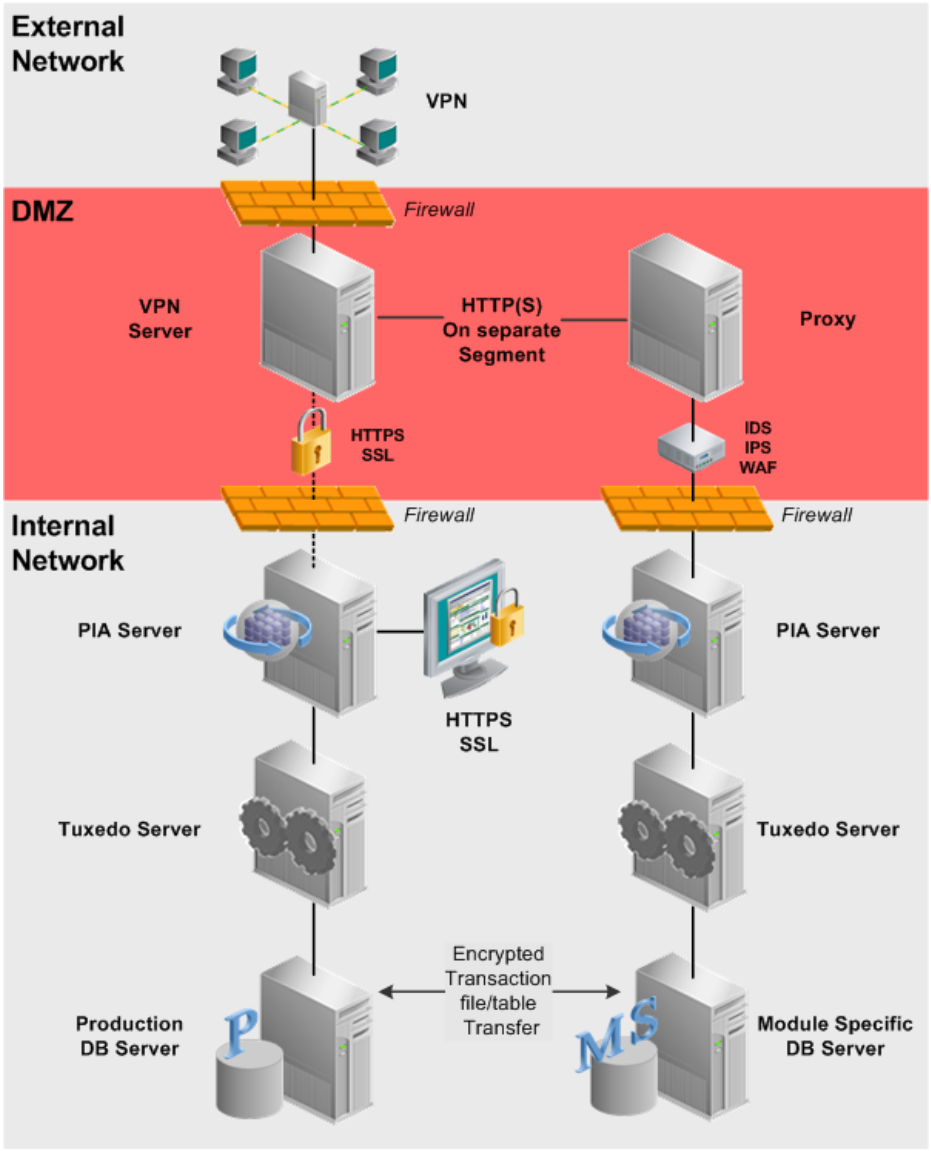
CANDIDATE GATEWAY

Self-service applications such as Candidate gateway can take advantage of decoupled systems, with periodic synchronization.

Example 3 is a dual stack with a complete separate instance for external access. Synchronization can be accomplished by any of the near real-time integration features or in batch mode.



Example 4 is similar to example 3 with dual stack. However, external access is accomplished here by means of VPN. Microsoft Windows provides a VPN client and secure access is relatively straightforward to implement.



Appendix B - Validation and Feedback

This section documents the real-world validation that this red paper has received.

We welcome feedback and discussion on the contents of this document.

CUSTOMER VALIDATION

Oracle PeopleSoft is working with PeopleSoft customers to get feedback and validation for this document. Lessons learned from these customer experiences will be posted here.

FIELD VALIDATION

Oracle PeopleSoft Consulting has provided feedback and validation for this document. Additional lessons learned from field experience will be posted here.

FEEDBACK

Please send any comments and suggestions to the PeopleTools Strategy peopletools_ww@oracle.com

Appendix C - Revision History

Authors

Oracle PeopleSoft Enterprise PeopleTools Development Team.

Revision History

1. December 2004 – Original Version
2. July 2010 – This Update