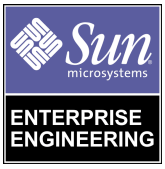
Building Secure N-Tier Environments

By Alex Noordergraaf - Enterprise Engineering

Sun BluePrints™ OnLine - October 2000



http://www.sun.com/blueprints

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300 fax 650 969-9131

Part No.: 806-7035-10
Revision 01, October 2000

Please
Recycle

Building Secure N-Tier Environments

Abstract

This article introduces recommendations for architecting and securing N-Tier environments.

The architecture presented here has been implemented successfully by several large organizations. In fact, this article could be a case study on how the architecture was implemented at various sites. The architecture has a modular design to enable different organizations to use only the components required for their specific environment.

This article highlights the fact that many organizations who rely on the Internet for their business have incorrectly architected their e-commerce environments. By implementing the following recommendations, a business may improve their architectures and provide improved availability and security.

Overview

N-Tier architecture is designed to use features of a multi tiered environment to increase security. Although the proposed architecture addresses RAS (Reliability, Availability, and Serviceability) issues, the primary focus of this paper is to build a secure environment. It is critical to design RAS features from the ground up to prevent compromising the security of the architecture.

The security enhancements discussed in this article include:

- Physical segmentation
- Automated OS installation
- Hardened and minimized OS installation
- Layered environment
- Dedicated network segments
- Host-based firewalls
- IP forwarding
- Encryption
- Backups
- Centralized logging
- Intrusion detection

Silver Bullet

The architecture discussed in this article is based on my experience within Sun Professional Services - Global Enterprise Security Service (GESS).

The motivation behind the development of a modular, robust, and securable architecture has been the speed at which organizations are developing and deploying e-commerce infrastructures. Although my primary focus is the overall security of the infrastructure, performance and manageability issues are important components.

By having a tested modular architecture as a building block for a new site, a development team can focus on other important issues.

Contrary to popular marketing hype, there is no one silver bullet that will solve all security issues. Although this article focuses on the main security issues, time does not permit all aspects to be discussed.

Primarily this article focuses on securing a highly available N-Tier architectures in which no component may be a single point of failure for the entire environment. Not all recommendations and/or requirements are applicable to all organizations.

N-Tier Description

A typical three tier architecture is usually described as having the following tiers:

1. Web Server / External Tier

2. Application Server Tier

3. Database Server Tier

These tiers include systems that provide a variety of services for example, the Web Server Tier almost always contain servers providing the following services:

- External Domain Name Servers (DNS)
- Simple Mail Transport Protocol (SMTP)
- File Transport Protocol (FTP)

In reality there will be additional tiers in an N-Tier environment. If all features described in this paper were implemented, there will be seven tiers:

1. Web Server / External Server Tier

2. Application Server Tier

3. Database Server Tier

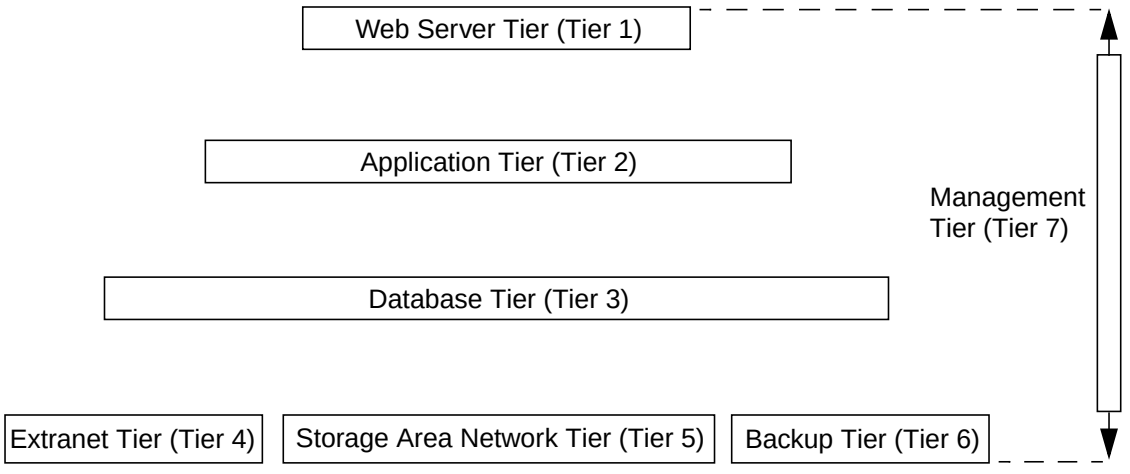
4. ExtraNet / Service Provider Tier

5. Storage Area Network Tier

6. Backup Tier

7. Management Tier

The following diagram illustrates the tiers:



The individual tiers are discussed as follows:

1 Web Server Tier

This tier should only contain systems that provide services directly to the Internet. This includes DNS, SMTP, HTTP protocols, and applicable HTTPS servers. Servers providing services to a system within the environment (such as the Lightweight Directory Access Protocol (LDAP)) must not be located within this tier. However, if LDAP services were provided directly to the Internet then locating an LDAP server on this tier would be appropriate.

Systems within this tier are among the most vulnerable to attack because they are exposed the public Internet. The security recommendations made in this article are of specific importance to these systems.

2 Application Server Tier

This tier contains all systems that communicate with the Web Server or Database Server Tiers. Additionally, any system the Web Server Tier must communicate with, but does not provide direct Internet services, must be located within this tier. The rule for system placement within the architecture is that a server should be located as far down in the N-Tier environment as possible. For example, if an LDAP server is used for authentication information within the Web Server tier, but is not accessed from the Internet—this server should be located within the next tier down (Application Server Tier).

Although systems located on this tier are not directly exposed to any external network, they have significant access permissions to the information stored in the backend database. Therefore, systems within this tier must also be secured.

3 Database Server Tier

This tier contains the crown jewels of the environment. This normally includes Relational Database Servers (RDBMS), internal DNS servers, and others. The servers located within this tier provide all services required by the Application Server and Database Server tiers. Although direct access from outside the environment is not provided for these systems, they too should be made secure.

4 Storage Area Network Tier

This tier has recently been added to the architecture. It has been included for two reasons. Firstly, the increasingly wide deployment of IP based Storage Area Network (SAN) devices. These devices or systems usually provide storage to a subset of servers located on the Database Server Tier, and therefore must be isolated.

The second (and primary) reason this tier was added was the popularity of outsourced SANs. In this model, storage is outsourced to a third-party which is typically (but not always) located in the same hosting facility as the architecture.

In this scenario, third-party vendors have access to network connections on critical servers in addition to all information stored within the SAN. Therefore, the SAN and its network traffic should be isolated from the rest of the network traffic by having its own network and dedicated connections to third party storage.

5 Backup Tier

Backing up critical data is crucial for system support, however, only those systems with changing data should be backed up. For example, if external web servers use dynamically generated content from the application servers, but contain no local dynamic application information, backups are not required. Obviously, the application and OS logs have to be uploaded, however, apart from the logs, there would be no other information that needs backing up.

The goal is to backup as few systems as possible, which reduces the number of tiers the Backup Tier must connect to. Each connection presents an intruder with an access mechanism into the contents of the Backup Tier. Access to the Backup Tier can provide the same information as the system being backed up.

6 ExtraNet / Service Provider Tier

Information and services from external sources are required in almost every e-commerce datacenter. The information may be as simple as stock information for a stock ticker, or it may be as complex as shipping inventory information. Regardless of the information required, it is essential to have timely and secure access to it.

Different organizations, service providers, and partners provide different access mechanisms to required information. Servers may need locating within the datacenter, or private leased lines may be used. In either case, the Extranet Tier is the location in which all connections (used by either the Database Server Tier or Applications Server Tier) must be located. If the information is to be used by other tiers within the architecture, then a separate ExtraNet Tier should be created to contain the necessary hardware.

7 Management Tier

The Management Tier is considered by some to be the most important and vulnerable tier within the architecture. This tier contains all network and server management software. All Simple Network Management Protocol (SNMP) servers are located within this tier. Additionally, terminal concentrators provide console access to each of the servers located in this tier.

The Management Tier is vulnerable because it provides administrators (and others) access to the environment. All software updates, debugging efforts, and patch updates for the environment originate from the Management Tier. This means administrative and operations staff must have access to this network in addition to local systems running window managers and laptop access.

Defense-In-Depth

The security concept of defense-in-depth can be readily applied to an N-Tier architecture. The premise is that no layer, device, or choke point should be a single point of security failure for the organization. By isolating and separating the servers and services in this manner, an intruder gaining access to the architecture will have several layers to traverse before gaining access to sensitive information. Intruders may access from within the organization, through an extranet connection, or the Internet.

Implementing separate networks and tiers can enhance the ability to detect intruders during an attempted breach of security.

Segmentation

The physical separation or segmentation of systems into tiers of systems that have similar services, security risks and exposure is critical to the overall security of the architecture. The grouping of systems is a fundamental building block of the modular N-Tier environment.

System Build Requirements

Each system within each tier must be secured. Because each system is exposed to different levels of risk, the security requirements for each system differs. Security requirements are based on the specific layer and how it connects to other systems/ layers. Systems that connect directly to the Internet are the most vulnerable. However, systems that connect to partner or outsourced networks must also be protected in the same manner as if they were connected directly to the Internet.

Each system must be secured—this process requires the following:

- Dedicated Functionality
- Hardening
- Host-based Firewall
- Minimization

Each of these points is discussed in further detail as follows:

Dedicated Functionality

First and most important, is dedicated functionality. It would be impossible to build a secure environment if, for example, the RDBMS is installed on a perimeter web server. This is a major security issue which violates one of the fundamentals of N-Tier architecture required for horizontal and vertical scalability.

Systems must be built around the services they provide to the environment. For example, an LDAP server should be constructed to offer LDAP services only to network interfaces that require access to it. Additionally, only encrypted user-access mechanisms such as SSH should be available. Such user-access mechanisms should only be available on network segments over which administrators and operators can gain access.

Systems built using this method will provide only one service to the environment. This arrangement will allow enhanced security through server customization. By dedicating hardware in this manner, the configuration of host-based firewalls rules, package listings, the OS, and applications can be simplified.

Hardening

Each system within the environment must be hardened. Security hardening is accomplished by modifying the default configuration of the Solaris™ Operating Environment. By default, many of the security features are disabled. These must be

enabled to improve the resilience of systems to unauthorized manipulation. For additional information on hardening a Solaris Operating Environment system, refer to the *Solaris Operating Environment Security* Sun BluePrints OnLine article listed in the References section. Additionally, scripts for hardening a Solaris Operating Environment system are available in the Toolkit described in the *JumpStart™ Architecture and Security Scripts* Sun BluePrint OnLine articles.

Host-based Firewall

Today, firewalls are common and are often referred to as the 'Silver Bullet' of security. Although firewalls can be used effectively within an N-Tier environment, they also have the potential to cause problems. Specifically, firewalls can adversely impact network availability and performance by becoming the choke points between network layers. Some organizations deploy firewalls between each tier of an N-Tier architecture—this may be done with the best of intentions, however, it can significantly affect the security and performance of the architecture.

Security and performance can be affected for several reasons. First, all traffic must go through this single system (or clustered firewalls in a HA configuration), therefore network traffic becomes susceptible. Additionally, the firewalls in a clustered arrangement must monitor the traffic flowing between tiers, making it difficult for network engineers to address scalability and availability requirements. This is most serious in an environment where a single point of failure is not permitted.

The second reason is the rulesets for the firewalls themselves. The protocols used by e-commerce applications frequently use dynamic ports on either the client or server side. Additionally, there are usually many services and protocols required—after these have been added to the environment, the firewall has so many ports open, its ability to function as a security device is severely compromised.

The third reason addresses the number of networks used in N-Tier environments. If firewalls are being used between network tiers on production networks, they must be used on the backup networks as well. Additionally, the management of networks is critical because as the number of firewalls grow exponentially they can become a management nightmare.

The fourth reason is service access. Many of the services provided by servers are only intended to be used on one network. However, most of the servers will be on at least three or more network segments. Because of this factor, unauthorized access can be made from the other networks—the firewalls located between the tiers may not protect against this.

However, there is a solution to the firewall issue. The solution has two parts. Firstly, any benefits the firewall can provide should be carefully evaluated before installation. Firewall placement should not be considered as routine as simply

checking a box. If there are no security benefits, then it should not be installed. Secondly, instead of locating firewalls between tiers, they may be more effective when installed on the individual servers themselves. In this way, firewalls can provide the fine level of granularity needed to provide services to specific networks, keep rulesets simple, and minimize network impact.

Minimization

Minimization is a process whereby any Solaris Operating Environment components not required are not installed on the system. A method of accomplishing this is presented in the *Solaris Operating Environment Minimization* article available from Sun BluePrints OnLine. By minimizing the number of Solaris Operating Environment components on each system, the number of components requiring hardening, patching, and configuring is reduced. The process of determining which packages are required can be time-consuming. Therefore, minimization is only recommended for systems particularly susceptible to possible security breaches. External web servers, firewalls, directory servers, and name servers are excellent candidates for this procedure.

Communication and IP Forwarding

The Solaris Operating Environment kernel has a setting which can enable or disable the forwarding of network traffic between network interfaces on a system. Within an N-Tier environment every system has many network interfaces—particularly when there are redundant network connections for each system.

IP forwarding must be disabled on all systems not explicitly functioning as a gateway or choke point. This imposes the requirement that systems must be physically connected to the networks they communicate with. At first glance this may seem to negatively impact security, however, it does the opposite in that it allows network segments to be isolated.

This isolation has the effect of forcing intruders to navigate through multiple layers to access sensitive information. However, for this method to be effective, the sensitive information must be isolated behind multiple layers. This is a primary reason why the N-Tier architecture has been segmented into small network tiers.

Network Flow

The goals and requirements for the security of networks will vary a great deal based on the availability and performance requirements of the infrastructure. For an environment that specifies no single point of failure, multiple network connections and equipment will be needed. Although this arrangement can be implemented, it presents specific requirements for managing traffic flows within the environment.

The use of a firewall as a choke-point has a significant impact on network infrastructure. Therefore, it is recommended that host based firewalls be used instead of choke-point based firewalls. There are, however, situations where a dedicated firewall is the correct solutions.

It is critical that firewalls only be used where there is a clear demonstration of added value. For example, on a hardened and minimized web server offering only HTTP and HTTPS to the Internet, there is little benefit in having a firewall. In fact, its only real use may be the restriction of services based on network interface(s). This may not be necessary if the application provides the required functionality.

The throughput of the network infrastructure should not be compromised because of security concerns—this means the location of firewalls must be carefully integrated into the network infrastructure.

Management issues for network infrastructure must also be considered. This is a major security concern due to the weakness of the SNMP based management traffic used to monitor networking devices. The management traffic should be kept on an isolated network not used for any other purpose.

System Configuration

By combining the principles outlined in the sections Defense-in-depth and Physical segmentation, the concept of a secured system begins to emerge. Systems built in this manner should be more secure because:

- Only services absolutely required are offered
- Services are only offered on network interfaces where absolutely required
- Systems are hardened
- Systems are minimized (where practical)
- Server-based firewalls are used throughout the environment

By combining these features systems will be more robust and resistance to unauthorized access then standard OS installations.

Network Segmentation

As previously described, an N-Tiered architecture has more than the three basic network tiers. The architecture described here has seven tiers to support the three tier application model.

Between each of the tiers there is a unique physical segment. Additionally, there is a segment between the Web Server tier and the Internet. The seven tier architecture model will comprise the following physical segments:

1. Internet — Web Server Tier
2. Web Server — Application Server Tier
3. Application Server Tier — Database Tier
4. ExtraNet Tier — Database Tier
5. Backup Tier — systems being backed up
6. SAN Tier — systems using SAN
7. Management Tier — all servers

The networks must be physically separate with respect to IP addresses, network devices, network interfaces servers, and network cables. Implementing this arrangement within the architecture can increase security of the environment because additional layers will have to be traversed to gain access to sensitive information. Each of the network segments between tiers is described as follows:

- Internet — Web Server Tier

Provides all systems on the Web Server Tier with a direct connection to the Internet.

- Web Server — Application Server Tier

As previously discussed, this network segment must use a different network interface and IP address range from any other.

All communication between the Web Server and Application Server Tiers will use this segment.

- Application Server Tier — Database Tier

As previously discussed, this segment must use a separate network interface and IP address range from any other.

All communication between the Application Server and Database Server Tier will use this segment.

- ExtraNet Tier — Database Tier

Until recently an extranet or network connecting to partners and/or service providers was uncommon, however, today it is uncommon to find an environment that does not have one. Because this type of network extends into other organizations these segments must be carefully isolated and controlled. Although many networks segments within an N-Tier architecture should not use firewalls, this network link may be an effective location to deploy a stateful packet filtering (SPF) based choke-point.

- Backup Tier — systems being backed up

The backup network is connected to systems requiring backup and uses separate network interfaces, switches, and IP addresses. Only systems requiring backup must be connected. For example, the perimeter web servers should have static configurations with almost no content. If this is the case, they will not require backing up. Ideally, this will be true of all systems within the Application Layer Tier.

- SAN Tier — systems using SAN

The SAN Tier must only connect to systems for which it provides services. Separate IP addresses, networking equipment, and network interfaces must be used.

- Management Tier — all servers

The management network is the most critical and vulnerable because it is used to update, manage, and monitor the environment. This network provides the highest level of un-secured services (i.e., window managers) and allows access all systems within the environment.

The recommended procedure for connecting the Management Tier to the systems within the environment comprises two parts. Firstly, physically separate and isolate the Management network connections to each system within the environment. However, even when separate networking equipment is used, the interconnection of all systems within one network violates many security requirements of the environment. Therefore, the Management network for each tier should be connected to separate interfaces on several gateway or firewall systems. Gateway systems separate the network traffic while still allowing required traffic to flow from the Management network to the individual systems.

Build Process

System installation and configuration should be as automated as possible (ideally, 100 percent). This includes OS installation and configuration, network configuration, user accounts, applications, and security modifications. When using the Solaris Operating Environment, the use of JumpStart software is recommended. Ideally, the

entire installation and configuration process should be automated. The Toolkit provides a framework and scripts to implement and automate most of the tasks associated with hardening and minimizing Solaris Operating Environment systems.

The previously described Gateway systems in the Management Tier are critical to the build process. The gateway systems, in addition to being firewalls, are also JumpStart boot servers. These systems are required on each network and provide the initial boot information for each server—this is required because the protocol used to provide a server with an IP address (Reverse Address Resolution Protocol RARP) is not a routed protocol.

Encryption

As many services as possible should be encrypted, this encompasses all user-interactive applications within the environment. These should include protocols such as TELNET, FTP, and r* —these should be replaced with an encrypted version such as SSH or SEAM. Additionally, the underlying network traffic may be encrypted through the use of SKIP or IPSec.

Non-interactive network based protocols should use encryption and strong authentication (where possible). When NFS or other services requiring Remote Procedure Calls (RPC) services are required, the secure RPC protocol should be implemented.

Backups

When setting up backups it is important to consider the information and how it will be stored. Security sensitive information such as user account and password information should be encrypted. Additionally, the encryption keys storing security information should be carefully managed.

Centralized Logging

The systems, network devices, and applications should be monitored—intrusions can only be detected if logs are created and monitored. Each system can produce a variety of logs from applications running on the system in addition to the logs

generated by the OS. At a minimum the logs generated by the OS must be reviewed on a regular basis. However, before they can be reviewed they must be generated. Therefore, each system within the environment must be configured to generate OS logs—which must be forwarded to a centralized log repository for systematic review. This centralized log repository must be carefully protected because it will contain a large amount of security related information—which intruders will want to eliminate.

The amount of information collected by this server will probably be considerable. The quantity is related to the number of servers and the level of log generation enabled. Even with the most basic of logging enabled, the quantity of traffic will be more than one person can effectively review. Therefore, the centralized monitoring station must have appropriate software installed to review the contents of the logs and provide an alert mechanism if any unusual entries are detected.

One other critical requirement for effective centralized logging is the use of Network Time Protocol (NTP) throughout the environment. In order to effectively reconcile log records from many different systems into one cohesive whole all systems must have synchronized clocks. This is most effectively done through the deployment of one or two time servers, on the management network, to which all other servers will synchronize.

Intrusion Detection

Intrusion detection systems are typically more effective when designed into the environment. In the segmented and layered architecture described here intrusion detection systems can function more effectively then if all network traffic flowed across a few shared networks. This is due to the well-defined nature of the networks in this architecture. Each network segment has some number of known protocols flowing across it. Based on these flows the intrusion detection system only has to look for unknown protocols and malicious traffic in those known protocols. This will simplify the task of the intrusion detection system thereby making it more effective.

References

Noordergraaf, Alex and Watson, Keith, *Solaris Operating Environment Minimization for Security*, Sun BluePrints OnLine, December 1999

`http://www.sun.com/blueprints/1299/minimization.pdf`

Noordergraaf, Alex and Watson, Keith, *Solaris Operating Environment Network Settings for Security*, Sun BluePrints OnLine, December 1999

`http://www.sun.com/blueprints/1299/network.pdf`

Noordergraaf, Alex and Watson, Keith, *Solaris Operating Environment Security*, Sun BluePrints OnLine, January 2000

`http://www.sun.com/blueprints/0100/security.pdf`

Noordergraaf, Alex, *Jumpstart Architecture and Security Scripts Toolkit - Part 1*, Sun BluePrints OnLine, July 2000

`http://www.sun.com/blueprints/0700/jssec.pdf`

Noordergraaf, Alex, *Jumpstart Architecture and Security Scripts Toolkit - Part 2*, Sun BluePrints OnLine, August 2000

`http://www.sun.com/blueprints/0800/jssec2.pdf`

Noordergraaf, Alex, *Jumpstart Architecture and Security Scripts Toolkit - Part 3*, Sun BluePrints OnLine, September 2000

`http://www.sun.com/blueprints/0900/jssec3.pdf`

Author's Bio: Alex Noordergraaf

Alex Noordergraaf has over nine years experience in the area of Computer and Network Security. As a Senior Security Architect in the Enterprise Engineering group of Sun Microsystems he is developing, documenting, and publishing security best practices through the Sun BluePrints OnLine program. Articles completed include recommendations on Solaris Security settings, Solaris Minimization, and Solaris Network settings.

Prior to his role in Enterprise Engineering he was a Senior Security Architect with Sun Professional Services where he worked with many Fortune 500 companies on projects that included Security Assessments, Architecture Development, Architectural Reviews, and Policy/Procedure review and development. In addition to providing billable services to customers he developed and delivered an Enterprise Security Assessment methodology and training curriculum to be used worldwide by SunPS. His customers have included major telecommunication firms, financial institutions, ISPs, and ASPs.