SUN™ MANAGED STORAGE SERVICES
SECURITY WHITE PAPER

May 2005

Table of Contents

Chapter 1

Overview

This document describes the various security processes and procedures used to address potential data security vulnerabilities related to the shared extranet connection between Sun and its customer used in the Sun℠ Managed Storage Service. This includes both external and internal threats. The data security approach described here covers a full cycle of prevention measures. One of the main premises of this paper is that while any extranet connection involves some level of security risk, the measures described here are sufficient to render the benefits of the extranet connection far greater than any downside risks.

Security is more than a purely technical issue, and must be a priority for all personnel that interact with the Sun Managed Storage Service. All customer and service delivery personnel must be trained to use best practices and effectively use tools that help enforce and automate the execution of security policies.

The paper also prescribes a layered approach to security. Firewalls comprise the exterior layer of security, and are applied to the network and assets attached to the network. Virtual Private Network (VPN) appliances comprise another layer and hardened operating systems on the management servers provide yet another layer. The multi-layer strategy means that any breach in security should be contained by one or more layers before it can compromise integrity of the system or its connections.

Chapter 2

Description of Sun℠ Managed Storage Services

The Sun Managed Storage Service provides customers with 24x7 management and monitoring of customer-owned SAN (Storage Area Network) environments. In addition, the customer has access to a web portal that details the operation of the SAN environment and provides a variety of reports covering availability, performance, capacity, etc. The Sun Managed Storage Service operations center provides a single point of contact for provisioning of SAN resources. The operations center also monitors customer SANs for any problems, including pending capacity issues, and initiates corrective actions while keeping the customer informed. All of this is performed using IT Information Library (ITIL) processes and best practices.

The Sun Managed Storage Service manages customers SAN equipment that are connected to a management LAN segment. The management LAN segment is isolated from the customer's other LAN segments and will have addressing assigned through the Sun Managed Storage Service. Management and monitoring of the management LAN segment will be performed over a VPN. This VPN will connect the management LAN segment to a Sun Managed Storage Service operations center LAN where management servers reside. The device used to establish the VPN will be a Juniper Networks Netscreen 5GT. The Netscreen 5GT will also have a connection to the production LAN segment where customer servers reside. This connection is needed in order to collect metadata on the customers file systems allocated from the SAN to customer servers. This metadata will be collected and processed for various reports for access through the Sun Managed Storage Service customer portal.

Chapter 3

VPN Connectivity

Figure 2.1 depicts the high level connectivity for the Sun Managed Storage Service. The VPN will utilize triple DES (3DES) encryption.

No connectivity between the customer's production LAN and the management LAN is permitted. The Netscreen 5GT will utilize policies that block all connections between those LAN segments. Connections from the customer's production LAN segments to the operations center will be limited to those servers that have a static route defined and a Mapped IP (MIP) entry on the Netscreen 5GT. An agent will reside on the production servers that will be polled by tools at the the operations center to collect metadata regarding the file systems allocated from the SAN on those servers. This data will consist of file system information (space used/available) as well as file metadata such as file names, file sizes, creation dates. The contents of all files and data remain on the customer's site and are not accessible by the tools used in the operations center.

The customer will be able to access a variety of reports and information on their equipment via a portal using encrypted connections over the Internet. This customer portal is not accessed over the VPN connection between the customer and the operations center. The HTTPS or SSL protocol will be used to encrypt information transmitted to and from the customer portal server.

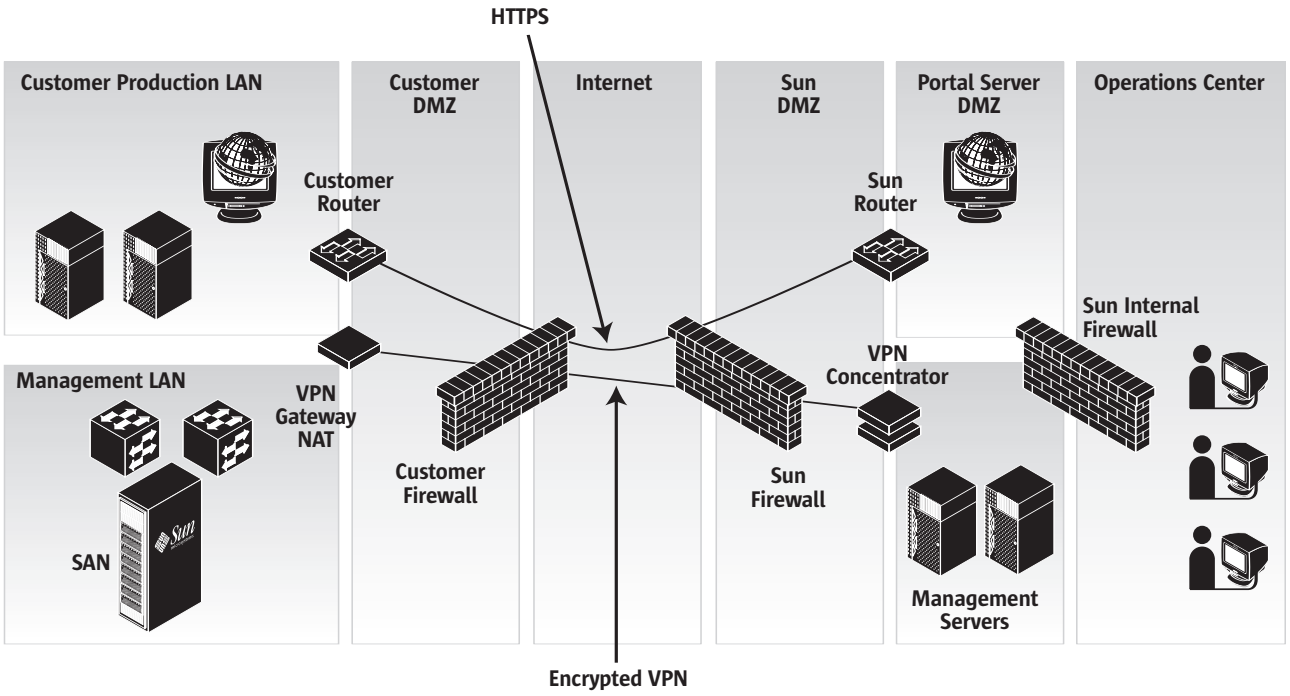

Figure 2.1

Customers will supply Sun Microsystems with an Internet connection and a public IP address that will be used by the VPN gateway to establish the VPN connection between the two sites. The customer will also provide an address on their production LAN that will be assigned to the Netscreen 5GT. The Netscreen 5GT will be configured to map the customer's

production LAN to addressing assigned by the operations center to prevent problems with overlapping addressing. The addressing on the Management LAN segment will be assigned by the operations center during initial installation of the service. Access to the log files on the Netscreen 5GT will be provided to the customer using syslog. The customer can also implement additional firewalls to enable capture all data going into and out of the VPN device.

Customers may deploy additional firewalls or segmentation of this extranet connectivity. The high level architecture defined in Figure 2.1 shows the basic architecture required for Sun Managed Storage Services.

Access into the customer's production LAN is limited to those devices running agents used by the Enterprise Storage Management (ESM) application. Access privileges are enforced by configurations on the VPN devices. The VPN devices use Mapped IP addressing to map the production server's real IP address to addressing assigned by the Sun Managed Storage Service operations center. In addition, a static route must be configured on the customer's server for traffic to be sent to the operations center. Only those servers with a static route and configured with MIP entries on the VPN device will be able to communicate with the management servers at the operations center.

The VPN connection will use a shared secret configured into the Netscreen 5GT device. No Internet connectivity other than over the VPN is permitted to the Netscreen 5GT. This includes Internet Control Message Protocol (ICMP) traffic to the public address assigned to the Netscreen 5GT. Network traffic is restricted by route entries as well as policies defined on the Netscreen 5GT device.

No connectivity between the management LAN segment and the customer's production LAN are permitted. This is enforced by policies defined on the Netscreen 5GT as well as the port mode used.

Connectivity between different customers is blocked not only by routing entries, but also by policies defined on the Netscreen at the operations center. Connectivity from the operations center to a customer location is restricted to a specific tunnel interface defined on the Netscreen at the operations center. Tunneling in combination with policy settings prevents possible spoofing attempts.

Chapter 4

Physical Security

Effective physical security of the Netscreen 5GT and the devices on the management LAN segment are also important in securing the network. The customer must provide effective physical security and limit access to physical assets only to essential personnel.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.co