STORAGETEK®

TECHNICAL BRIEF

Remote Managed Storage services security

APRIL 2004

Remote Managed Storage services security

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

StorageTek® Remote Managed Storage services offering is designed to offer StorageTek customers the most flexibility in managing their storage environment while achieving SLAs (Service Level Agreements) for various services such as backup and restore. StorageTek meets these SLAs with a combination of skilled personnel working 24x365 and a secure, fault-tolerant infrastructure that incorporates the Internet as a transport mechanism. The imminent requirements, initiatives and mandates such as the Health Insurance Portability and Accounting Act (HIPAA) will further emphasize the importance of security and high-availability in managing an enterprise storage environment. This paper provides an overview of the methods used in achieving security and fault-tolerance in the StorageTek Remote Managed Storage. StorageTek understands the dynamic nature of security and is committed to an ongoing effort to achieve the highest level of security in an effort to gain, and maintain, customer trust.

2 SETTING THE STAGE

The Remote Managed Storage storage operations center provides nonstop monitoring and management of all customer storage environments. As a result, the underlying service delivery infrastructure is challenged to achieve high-availability by helping fault-tolerance at the server and communications level. In addition, the high-availability goal forces the infrastructure to be capable of a quick failover in the event of a failure without manual intervention.

Before getting into the details of the Remote Managed Storage infrastructure, it is important to identify the components and the roles they play. **Figure 1** (see below) depicts all components of this infrastructure:

> Storage communication appliance

- StorageTek asset deployed at the customer premise to allow the storage operations center to monitor and manage the customer's storage infrastructure
- Comprised of servers, routers and switches in both HA (high-availability) and non-HA offerings
- HA offering includes dual servers, routers and switches

> Administration and operations processing system (AOPS)

- The AOPS is populated by servers to manage and monitor the storage communication appliances using off-the-shelf applications for SNMP (Simple Network Management Protocol) monitoring, event correlation and configuration management to aid in problem isolation and resolution
- Two identically configured components, AOPS-East and AOPS-West
- AOPS-East and AOPS-West are in different locations served by different ISPs

> Storage operation center

- Nonstop operation manned 24x365
- Monitors AOPS-East, AOPS-West and SCA availability
- Monitors customer SAN environment
- Fulfills customer service requests
- Storage operations center personnel exclusively storage experts.

The strategic security goals of this infrastructure are:

> To protect the customer, the AOPS and the storage operations center as an enclave, with a rigorous perimeter using physical security, VPN and firewall-risk-reduction technologies and policies.

> To help ensure that privacy goals related to customer data are achieved by limiting storage operations center access to customer meta-data only.

> To prohibit customer-to-customer traffic.

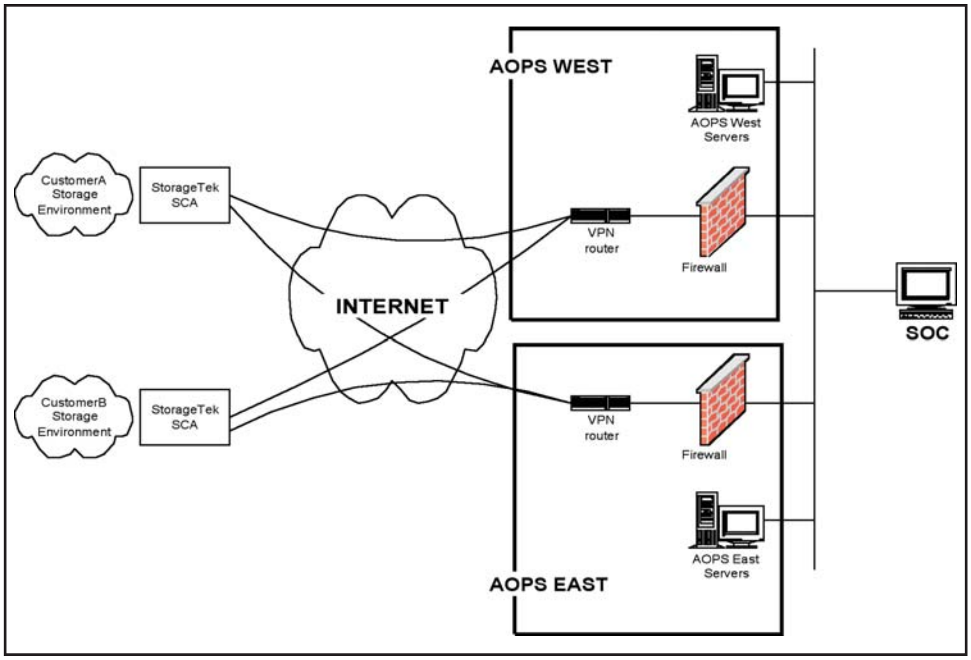

Figure 1. Components of the Remote Managed Storage infrastructure.

3 THE PROBLEM… THE SOLUTION

StorageTek is committed to achieving and maintaining the trust of its customers. Furthermore, StorageTek understands the importance of meeting the customer's security policies relevant to data center outsourcing and remote access. To achieve compliance with these policies, StorageTek provides documentation explicitly stating the specific ports, protocols and destination addresses required by Remote Managed Storage. StorageTek is also readily available to discuss and further review the security elements of the service delivery infrastructure.

In the context of this white paper, customer trust is accomplished by maintaining a perimeter built with a combination of physical and electronic security measures deployed in a layered approach. Access to the storage operations center, AOPS-East and AOPS-West, is limited to authorized personnel only and protected by 24x365 card key access as well as video surveillance. All access is logged for the potential purpose of aiding a forensic effort.

As shown in **Figure 1**, each storage communications appliance, configured for high-availability, has two connections to the AOPS infrastructure. These two connections are a pair of IPsec VPNs (IP Security Virtual Private Networks), with one VPN terminating in AOPS-East and the other in AOPS-West. The IPsec VPNs are configured for ESP (encapsulating security payload) in tunnel mode with Diffie-Hellman Group 5 and Perfect Forward Secrecy for key management, 3DES encryption and SHA-HMAC for authentication. The tunnel authentication phase of the AOPS-to-SCA VPN uses a pre-shared password which is unique per customer site. These passwords are random strings, changed on a regular basis and stored in an encrypted file on the SOC server with access to this file limited to authorized personnel.

Over the two tunnels between an SCA and the AOPS, a routing protocol is configured with a weighted preference thereby providing the ability to failover quickly and automatically. All routing protocol communications are authenticated by an MD5 signature and, to aid the goal of prohibiting customer-to-customer traffic, the storage communications appliance only learns a new default route. To help ensure the denial of customer-to-customer traffic, the AOPS VPN router blocks such traffic via access control lists.

The storage communications appliance routers are configured to monitor traffic from the storage communications appliance LAN for intrusion attempts matching one of 59 attack and information gathering signatures. Traffic that originates at the storage communications appliance and is destined to the AOPS is limited to syslog, TACACS (Terminal Access Controller Access Controller System), NTP (Network Time Protocol) and SNMP traps and informs. The control of storage communications appliance originated traffic is performed at both the AOPS VPN router via access control lists and rules on the AOPS stateful firewall.

All access to the storage communications appliance and AOPS network devices is controlled by both access control lists and two-factor user authentication using TACACS to communicate with the RSA (Rivest-Shamir-Adleman) ACE (Advanced Computing Environment) server. Authorized personnel are provided RSA key fobs that provide the one-time password in conjunction with a PIN known only to the user. User access to these devices is logged via RADIUS (Remote Access Dial-In User Service) accounting records providing a detailed audit trail. In addition, remote access to these devices is limited to encrypted methods such as SSH (Secure Shell).

It is also noteworthy to point out that the Cisco configurations for both the SCA and AOPS routers and switches are significantly influenced by security guidelines such as those published by Cisco Systems and the National Security Agency. The storage communications appliance servers are all configured with a hardened operating system build eliminating and/or disabling any unnecessary services not required by the storage operations center.

All storage communications appliance and AOPS components log various activities and events to central AOPS logging servers. Each logged message is time-stamped using an NTP-derived clock to help make sure events are synchronized for aid in problem isolation efforts.

4 ACCESS TO CUSTOMER ASSETS AND DATA

The customer has full control over which assets are visible to the storage operations center with visibility controlled by customer firewalls, router access control lists, etc.

The customer data visible to the storage operations center is limited to data pertinent to satisfying a requested data restoration or storage network management. The storage operations center will have access to all meta data regarding backups for use in performing restores such as file system names/locations as well as file names, dates, sizes and locations on all hosts that have had backups performed in the managed environment. For storage network management the storage operations center will have access to disk geometries, LUN security and various storage interconnects.

The storage operations center is contractually obligated to provide management capability of the backup environment and/or storage network and to not view any customer data contained therein. This includes restoration of customer data as well as providing storage to any systems other than that requested by the customer.

STORAGETEK®

ABOUT STORAGETEK®

Storage Technology Corporation (NYSE: STK), a $2 billion worldwide company with headquarters in Louisville, CO, has been delivering a broad range of storage management solutions designed for IT professionals for over 30 years. StorageTek offers solutions that are easy to manage, integrate well with existing infrastructures and allow universal access to data across servers, media types and storage networks. StorageTek's practical and safe storage solutions for tape automation, disk storage systems and storage integration, coupled with a global services network, provide IT professionals with confidence and know-how to manage their entire storage management ecosystem today and in the future.

StorageTek products are available through a worldwide network. For more information, visit www.storagetek.com, or call 1.800.275.4785 or 01.303.673.2800.

WORLD HEADQUARTERS

Storage Technology Corporation
One StorageTek Drive
Louisville, Colorado 80028 USA
1.800.877.9220 or 01.303.673.5151