The Scientific Consulting Group, Inc.

System Design Document

for the

SCG Secure Cloud System

Version 1.4

May 19, 2016

The Scientific Consulting Group, Inc.
656 Quince Orchard Road
Suite 210
Gaithersburg, MD 20878

System Design Document Approval

The System Design Document for the SCG Secure Cloud (SCGSC) system must be approved by the SCG President, Vice President of Administration, and Information Technology (IT) Director. The undersigned acknowledge that they have reviewed the System Design Document for the SCGSC system and agree with the information presented herein. The IT Director and SCG President will review this document at least once every three (3) years and revise the document as necessary to address system/organizational changes to the SCGSC system. Changes to the System Design Document will be coordinated with, and approved by, the undersigned, or their designated representatives.

5/19/16

Beverly J. Campbell
President

DATE

5/19/16

Stacy E. Philipson
Vice President of Administration

DATE

5/19/16

Chuck C. Lee
Director of Information Technology

DATE

Document Information and Revision History

Document Owners	
SCG President	
Name	Beverly J. Campbell
Contact Number	301-670-4990 (W); 301-461-1109 (C)
E-mail Address	bcampbell@scgcorp.com
SCG Information Technology Director	
Name	Chuck Lee, Information Technology Director
Contact Number	301-670-4990 (W); 301-366-3273 (C)
E-mail Address	clee@scgcorp.com
SCG Vice President of Administration	
Name	Stacy Philipson
Contact Number	301-670-4990 (W); 301-742-5954 (C)
E-mail Address	bcampbell@scgcorp.com

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	2/20/15	C. Lee	Draft System Design Document
1.1	2/23/15	B. Campbell	Edited and made modifications throughout the document
1.2	2/25/15	B. Campbell/ R. Blackman	Edited and made modifications throughout the document
1.3	3/4/15	B. Campbell/C. Lee	Made minor modifications throughout the document
1.4	5/19/16	B. Campbell	Made minor modifications throughout the document

This record shall be maintained throughout the life of the document. Each published update shall be recorded. Revisions are a complete re-issue of the entire document. The version number's decimal (minor) portion here and on the cover page is updated for each revision. The version number's integer (major) portion will be updated at each time a full Security Assessment and Authorization is performed.

Table of Contents

List of Tables

List of Figures

1. Project Overview

1.1 Document Scope

The scope of this document is limited to the SCG Secure Cloud (SCGSC) system and applications hosted within.

1.2 Document Purpose and Dissemination

This document provides an architectural overview of the SCGSC system. The document is intended to capture and convey the significant architecture of the system and depicts the technical aspects of the system components and design decisions that have been made in developing the SCGSC system. This document is disseminated to the SCG IT staff who have access to and are responsible for the SCGSC system and it is posted on the SCG Intranet in a read-only format to facilitate easy access by SCG employees.

1.3 SCGSC Project Overview

The SCGSC system is created to support a contract awarded to SCG to provide Support for National Information Clearinghouses and Campaign-Focused Programs for the National Institute of Diabetes and Digestive and Kidney Diseases' (NIDDK) Office of Communications and Public Liaison, in Bethesda, Maryland. This contract enables NIDDK to ensure that the science-based knowledge gained from NIDDK-funded research is imparted to NIDDK target audiences, including health care providers and the public for the direct benefit of patients and their families. Based on the statement of work for the contract, the SCGSC System serve as an infrastructure hosting capability for applications and services that include: the Inventory Tracking System for the NIDDK Clearinghouses, Secure Online Ordering Catalog, Mailing List Database, Websites, Videos, and other items.

The SCGSC system is the underlying infrastructure that hosts primary systems that support the NIDDK Clearinghouses and national education campaigns. It will be used by SCG, NIDDK, and other users on a daily basis. This system is continuously used during business and non-business hours, providing the hosting capabilities that support health information that supports NIDDK's mission. The confidentiality, integrity, and availability of the SCGSC system is critical, i.e., ensuring that data are only received by the persons and applications that they are intended for, that data are not subject to unauthorized or accidental alterations, and that the resources are available when needed.

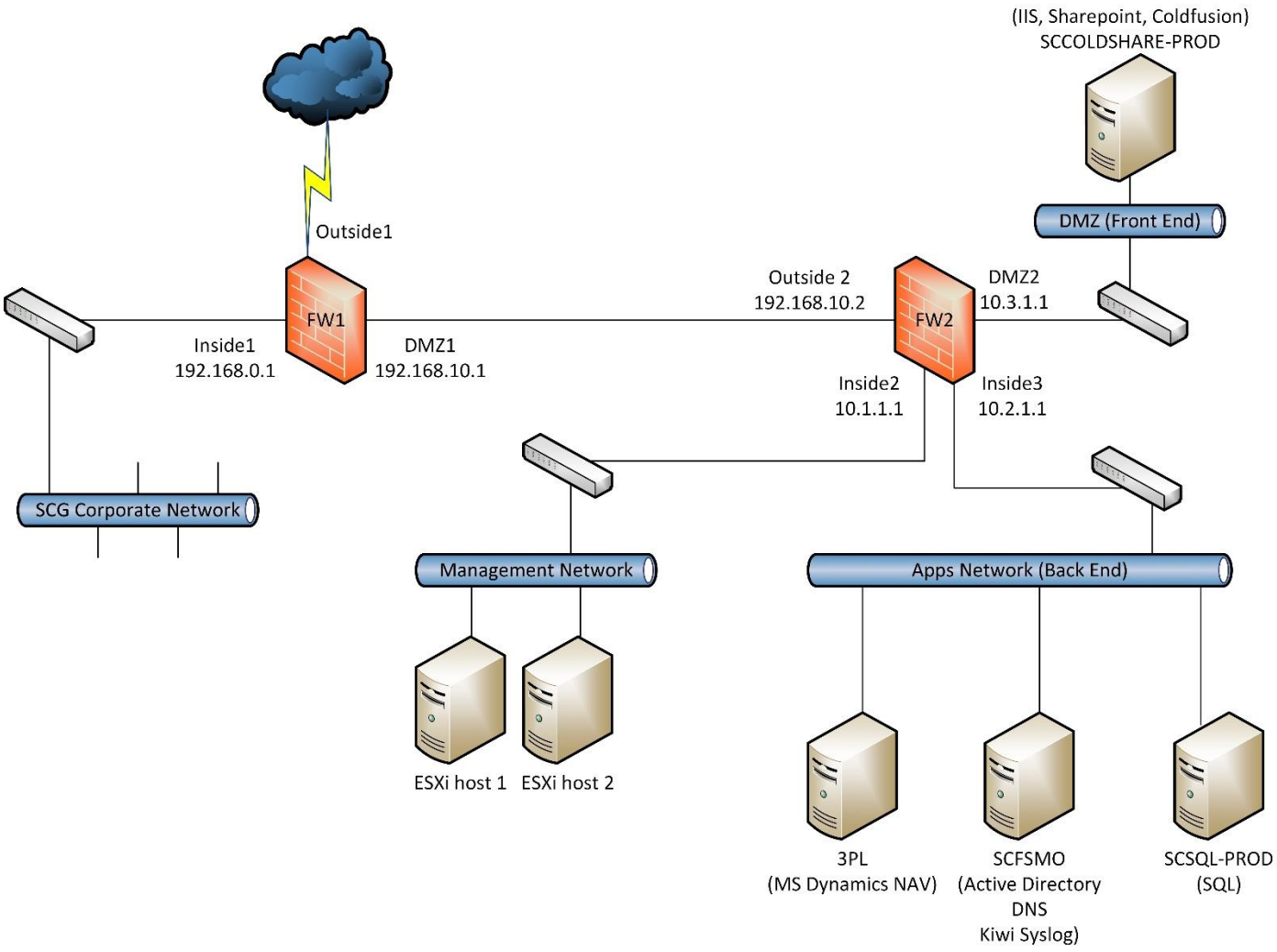
SCG adheres to the security design philosophies and principles outlined in NIST Special Publication 800-27 Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.

2. Solution Concept

2.1 SCGSC Overview

An overview of the SCGSC system is presented in Figure 1.

Figure 1. SCGSC System Overview



Developers/Administrators need to access Inside2 and Inside3 to provide regular administrative management for the IT assets that are connected to that network segment. Access to these IT assets is controlled by:

1. Network Address Translation (NAT) rules
2. Limited to group of Internet Protocols (IPs)
3. Control is done manually by clicking On/Off as needed

Internet/public users need access to DMZ2 (IIS/Sharepoint/Coldfusion) to permit interaction with NIDDK hosted applications and services. Interactions with these applications, services, and websites is permitted by:

1. One to one NAT rules on FW1 and FW2
2. Only http and https (port 80 and 443) protocols are allowed

All servers and hosts in DMZ2, Inside2, and Inside3 need to communicate to Inside1

1. To report back to Symantec Endpoint Protection Suite Enterprise server for updates and alerts
2. To receive email alerts from Kiwi Syslog
3. To backup all virtual servers

All servers in DMZ2 and Inside3 need access to Outside 1 for Windows updates. Control is done manually by clicking On/Off as needed.

The following is a summarization of the configured boundary protections that are applicable to this system:

FW2 Rules

DMZ2 → Oustide2

DMZ2 –X– Inside2

DMZ2 –X– Inside3 (specific ports allowed only)

Inside2 –X– DMZ2

Inside2 –X– Outside2

Inside2 –X– Inside3

Inside3 → Outside2

Inside3 –X– DMZ2

Inside3 –X– Inside2

Outside2 default route to DMZ1

NAT from Inside2 and DMZ2 to Outside2 (static NAT pool one to one)

Outside2 NAT (one to one) to Inisde2 for VSphere client

FW1 Rules

Inside1 → Outside1 (default)

Inside1 → DMZ1

Outside1 → Inside1

Outside1 → DMZ1 (one to one NAT to IIS/Sharepoint/Coldfusion server)

DM1 default route to Outside1

Outside1 default route to Internet

Dynamic NAT (pool) from Inside1 to Outside1

Static NAT (one to one) for certain Inside1 servers

No NAT from Inside1 to DMZ1

2.2 System Service Description

A brief description of the SCGSC system services is provided in Table 1.

Table 1. SCGSC System Services

Services	Functions
ESXi host 1 ESXi host 2	Runs the virtual machines (VMs) with high availability (fault tolerance with minimal downtime)
Sharepoint	Supports the operation of hosted Sharepoint applications
Coldfusion	Supports the operation of hosted Coldfusion applications
IIS	Supports web publishing (websites)
DNS	Resolves domain names and IPs
Active Directory	Authenticates users and provide access control services based upon Microsoft group membership(s)
Kiwi Syslog	Collects system logs and generate reports
Cisco IPS	Monitors and prevents intrusions and viruses
BackupExec	Runs Symantec backup software
Symantec Endpoint Protection Suite	Provides the A/V protection services for malware, malicious code, code execution at runtime (i.e., memory protection), and limited incident response notifications
Microsoft Dynamics NAV	Enterprise resource planning (ERP) software suite

2.3 System Interfaces

The SCGSC interfaces and their functions are identified in Table 2.

Table 2. SCGSC System Interfaces

Interfaces	Functions
Inside1	Management, backup, email, and Symantec Central Server
Inside2	Managing ESXi hosts/VMs and backup

Interfaces	Functions
Inside3	Back end application network for database, domain controller, collecting system logs, and generating reports
Outside1	Connect to Internet
Outside2	Connect to DMZ1
DMZ1	Connect to Inside1 and Outside1
DMZ2	Front end application network hosting websites

2.4 System Operation

The SCGSC devices and their applicable software/firmware versions are listed in Table 3.

Table 3. SCGSC System Operation

Devices	Firmware/Software Version
SCSQL-PROD	Windows 2008 R2 SP1
SCCOLDSHARE-PROD	Windows 2008 R2 SP1
SCFSMO	Windows 2008 R2 SP1
3PL	Windows 2008 R2 SP1
VMWare ESXi Host 1 VMWare ESXi Host 2	6.0 update 2
Cisco 5512-X	ASA ver. 9.5(2)5
Cisco 5515	ASA ver. 9.3(1)
Cisco 2960	15.0(2)SE7
Netgear FS524S	NA
Netgear GS108	NA
Cisco SG110D-08	NA
HPE NAS 1450	Windows Storage Server 2012 R2
APC Smart-UPS 3000VA	NA

2.5 System Roles

The roles of the SCGSC devices are defined in Table 4.

Table 4. SCGSC System Roles

Devices	Roles
SCSQL-PROD	Database, naming, centralized logs, and providing foundational services and capabilities in support of user authentication actions controlled by hosted applications
SCCOLDSHARE-PROD	Provides directed web access to hosted web applications that are stored within the SCGSC
SCFSMO	Domain controller provides foundational services and capabilities in support of user authentication, Active Directory, and DNS
3PL	Provides access to ERP software suite in support of call center and clearinghouse operations
VMWare ESXi Host 1 VMWare ESXi Host 2	Hosts virtual machines (VMs) with high availability (fault tolerance with minimal downtime)
Cisco ASA 5512-X	Controls and routes traffic and prevents intrusion and viruses for SCGSC System; maps internal network to external
Cisco ASA 5515	Controls and routes traffic and prevents intrusion and viruses for Corporate System; maps internal network to external; also provides additional security for SCGSC System
Cisco 2960	Routes traffic to privileged user network (back end application network)
Cisco SG110D-08	iSCSI connection from hosts to NAS device
Netgear FS524S	Routes traffic to management network
Netgear GS108	Routes public facing internet traffic to the DMZ2 network
HPE NAS 1450	Storage for virtual machines (VMs)
APC Smart-UPS 3000VA	Uninterruptible power supply

3. Software Logical Component Description

Applications on IIS/Sharepoint/Coldfusion server collect/query data that are stored in SCSQL-PROD. The responsibilities of the SCGSC are limited to providing the infrastructure services required in support of application to data tier read-write operations. The specific operations for data read, write, and modify are controlled by the security architecture and within the security boundary of each individual application or system that is hosted within the SCGSC; however it should be noted that the actual security control and boundary of each independent application are subject to the Authority to Operate (ATO) for those applications.

The SCGSC solution provides limited data collection capabilities that can be used to augment the secure operations of NIDDK provided applications, systems, and services. Some of these data collection activities include:

All Windows logs and Cisco firewall Intrusion Prevention System (IPS) logs are collected by Kiwi Syslog, where reports can be run and analyzed.

Symantec Endpoint Protection Suite Enterprise 2015 updates its definitions and status to and from the Symantec server located in the corporate network through a secure port (8014).

Cisco IPS updates its definitions directly from Cisco using the IT Director's login credentials. Alerts are sent directly to the IT Director's e-mail address.

The software components that comprise the SCGSC system include:

- **VMWare Host** – VMWare ESXi version 6.0 Update 2
- **SQL Database Server** – Windows Server Operating System version 2008 R2 with SQL Server 2012 Standard (x64) SP2 Symantec Endpoint Protection Suite, and Kiwi Syslog 9.4.1
- **Web Server** – Windows Server Operating System version 2008 R2 with Microsoft IIS 7.0, Sharepoint Foundation 2010, Coldfusion 9, , Symantec Endpoint Protection Suite
- **3PL** - Windows Server Operating System version 2008 R2 with Microsoft Dynamics NAV and , Symantec Endpoint Protection Suite
- **SCFSMO -** Windows Server Operating System version 2008 R2 with Symantec Endpoint Protection Suite

3.1 Logical Deployed Software Architecture

The logical deployed SCGSC software architecture is depicted in Figure 2 and the logical application data flow in Figure 3.

Figure 2. SCGSC Solution Architecture

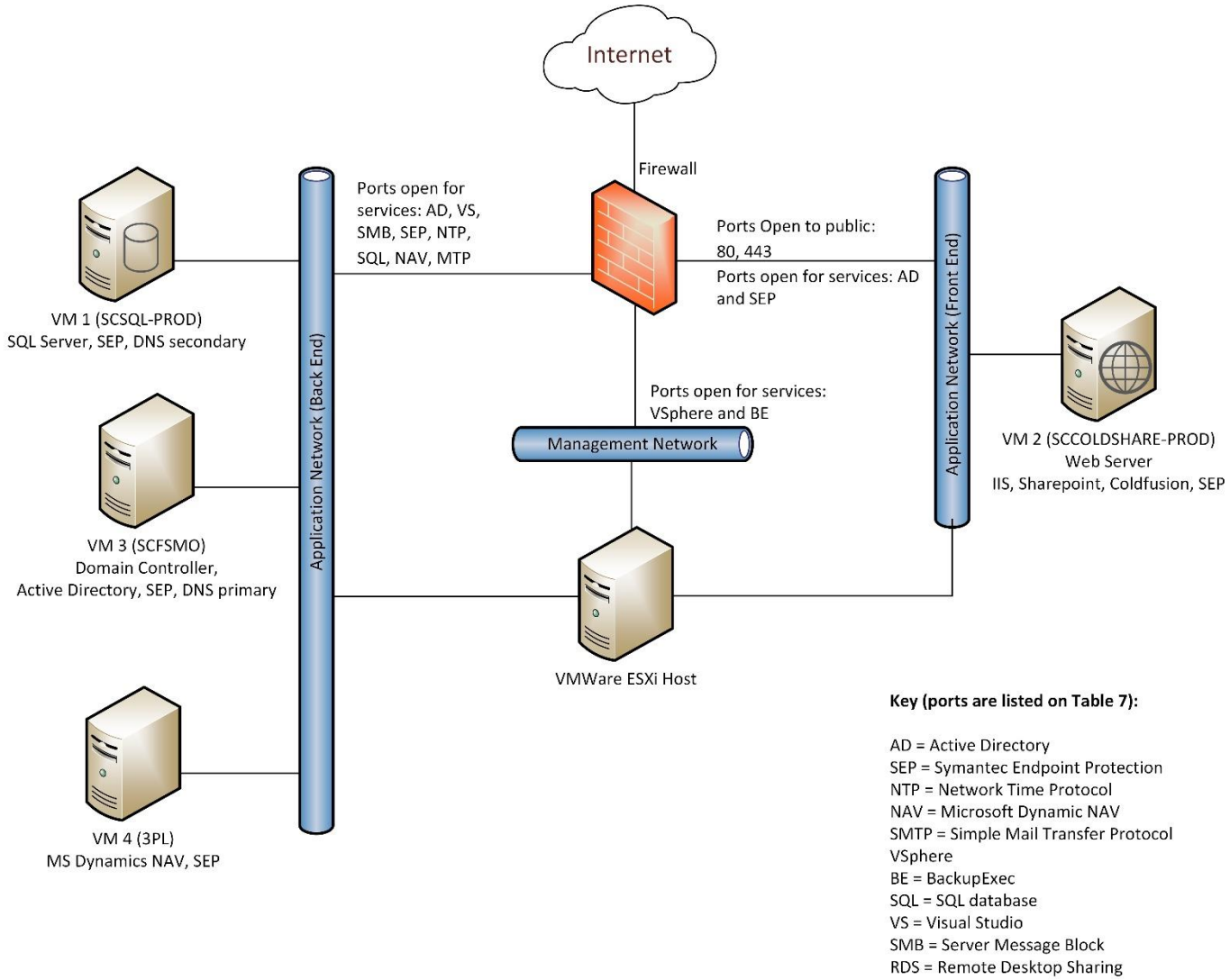
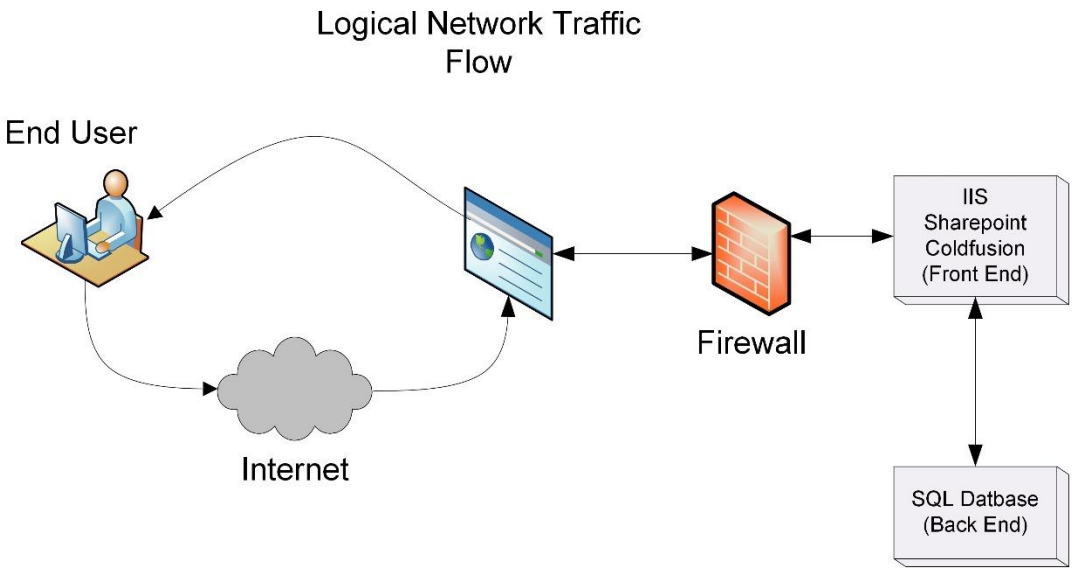


Figure 3. Detailed Logical Application Data Flow



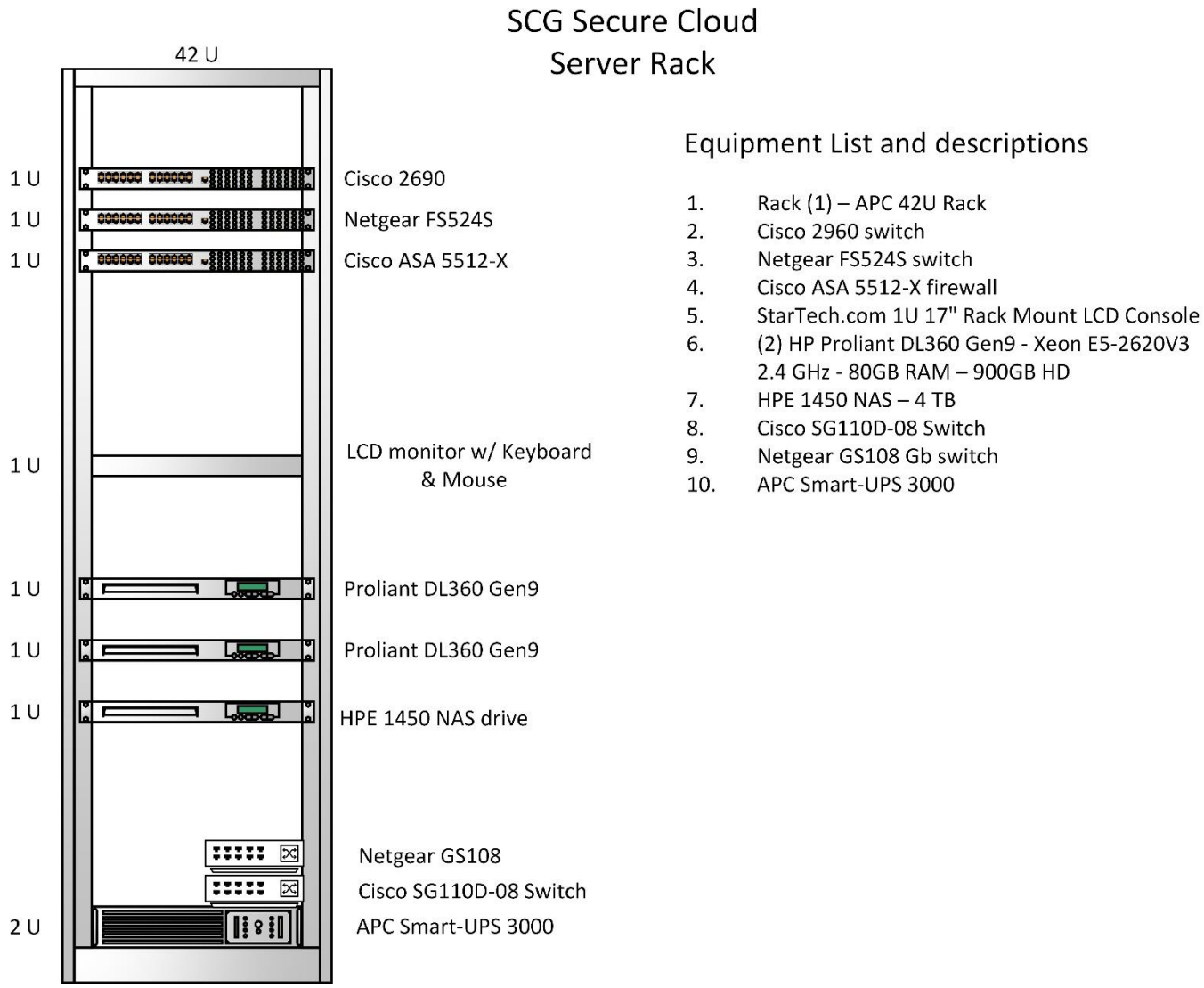
The logical application data flow of the SCGSC permits users of hosted applications and services from NIDDK to access those applications through a protected system edge (i.e., Firewall in Figure 3 above). The firewall protects and controls the flow of traffic to the applications that are hosted on the front end Web Server (see Figure 2) and the back end SQL Server (see Figure 2). The flow of traffic for Public interfaces is appropriately secured to meet the security requirements for interacting with the SCGSC, commonly using Port 80 (HTTP) and 443 (HTTPS). The target for this logical data flow is the Virtual Machines that is located behind the secure firewall in the public facing DMZ2.

The nature and security of the traffic that is supported by the SCGSC is controlled by the security demands of the hosted NIDDK application or service. The scope and boundary of the logical data flow control for the SCGSC is limited to an appropriate configuration and proper security protections required from an infrastructure hosting capability/service.

4. System Physical Description

The SCGSC system contains the equipment identified in the rack configuration presented in Figure 4.

Figure 4. SCG Secure Cloud Equipment



4.1 System Operational Service Model/Design

SCGSC is isolated from the SCG corporate network with a physical firewall and appropriate configured firewall rules that isolate that traffic through dedicated network interfaces. The system supports backup system that exists both at the primary and alternate sites.

4.2 Physical Server Operations

There are two physical server in SCGSC.

4.3 Workstation Operations

The SCGSC system does not have any workstations.

4.4 System Hardware Architecture

The SCGSC system hardware is listed in Table 5 and the technical architecture diagram is provided in Figure 5. The system component connectivity is depicted in Figure 6.

Table 5. SCGSC System Hardware and Component Inventory

Configuration Item Name	Item Description	Type	Function	Software/Version
VHOST1	HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, RAID 5 Serial #: MXQ44002RJ	Hardware	Server	VMware VSphere ESXi 6.0 update 2
VHOST2	HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, RAID 5 Serial #: MXQ4400250	Hardware	Server	VMware VSphere ESXi 6.0 update 2
SCSQL-PROD (VM 1*)	Virtual Machine Serial #: NA	Software	Database Server	Windows 2008 R2 Enterprise (x64) SP1 SQL Server 2012 Standard (x64) SP2 Symantec Protection Suite Enterprise 2015 DNS (secondary) Kiwi Syslog
SCCOLDSHARE-PROD (VM 2*)	Virtual Machine Serial #: NA	Software	Web Server	Windows 2008 R2 Enterprise (x64) Microsoft IIS 7.0 ColdFusion 9 SharePoint Foundation 2010 Symantec Protection Suite Enterprise 2015
SCFSMO (VM 3*)	Virtual Machine Serial #: NA	Software	Domain Controller	Windows 2008 R2 Enterprise (x64) DNS (primary) Active Directory Symantec Protection Suite Enterprise 2015
3PL (VM 4*)	Virtual Machine Serial #: NA	Software	Webserver	Windows 2008 R2 Enterprise (x64) MS Dynamics NAV Symantec Protection Suite Enterprise 2015

Configuration Item Name	Item Description	Type	Function	Software/Version
SCGSCSW01	Cisco 2960 Manageable Switch Mode3l: WS-C2960-48TC-L Serial #: F0C1148U3EG	Hardware	Routes traffic to non-privileged user network (internet to apps)	15.0(2)SE7
SCGSCSW02 (Unmanaged Switch)	Netgear FS524S 24-Port Switch Serial #: FS5A1C003773	Hardware	Routes traffic to management network	NA
SCGSCSW03 (Unmanaged Switch)	Netgear GS108 8-Port Gigabyte Switch Serial #: 1DR16B3Y0024E	Hardware	Routes traffic to the DMZ2 network	NA
SCGSCSW04 (Unmanaged Switch)	Cisco SG110D-08 8-Port Gigabyte Switch Serial #: DNI20120CF0	Hardware	iSCSI connection from hosts to NAS device	NA
SCGSCFW02	Cisco ASA 5512-X Model: ASA 5512v3 Serial #: FTX185110VX	Hardware	Filters traffic and maps internal network to external	Cisco Firewall ASA 9.1.2
SCGSCIPS	Added module for Cisco ASA 5512-X Model: ASA 5512v3 Serial #: NA	Hardware/ Software	Continuously prevents intrusion, Trojans, and hackers	IME ver. 7.3
SCGSCUPS	APC Smart-UPS 3000VA Serial #: AS1350133484	Hardware	Uninterruptable Power Supply	NA
SCNAS01	HPE 1450 NAS	Hardware	Host Virtual Machines (VMs)	Windows Storage Server 2012 R2
SCGSCRACKCONV	Startech LCD Serial #: E071X4A40184	Hardware	Display, keyboard, mouse	NA

* VM 1, VM 2, VM 3, and VM 4 are virtual machines that are an emulation of a particular computer system that resides in the memory of the physical host.

Figure 5. SCGSC System Architecture Diagram

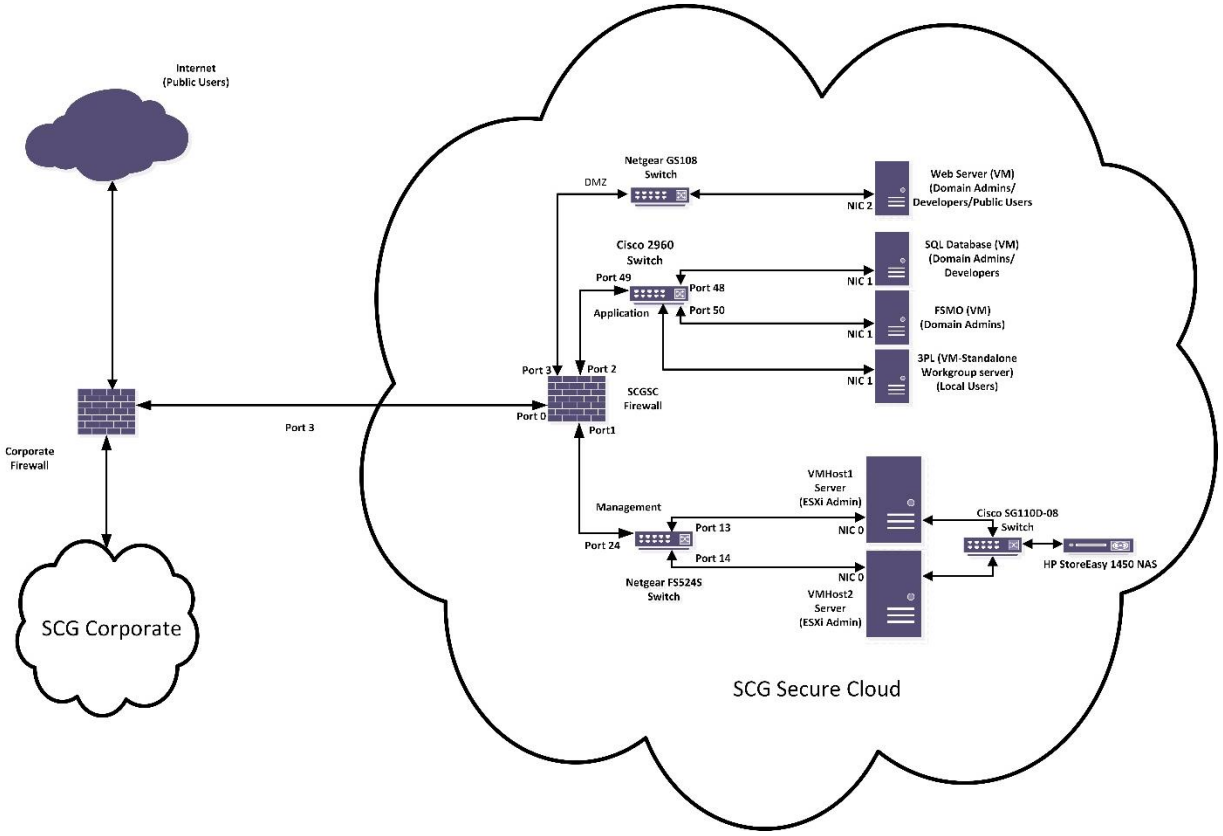
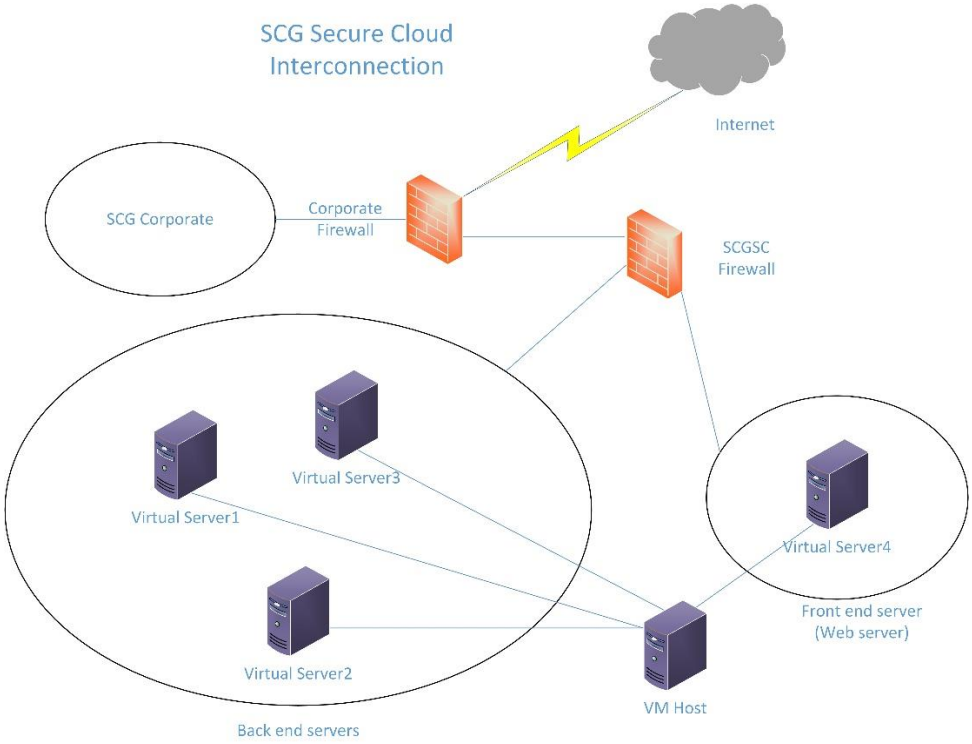


Figure 6. SCGSC System Component Connectivity



4.4.1 Solution Operating Environments

The SCG Secure Cloud system has two host servers consisting of two HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, RAID5 running VMWare VSphere ESXi 6.0 update 2.

The VM Host supports the operations of four virtual machines which are as follows:

- VM 1 (SCSQL-PROD) – Windows 2008 R2 Enterprise (x64), SQL Server 2012 Standard (x64) and a local secondary DNS Server, and Kiwi Syslog
- VM 2 (SCCOLDSHARE-PROD) – Windows 2008 R2 Enterprise (x64), Microsoft IIS, Coldfusion 9, and Sharepoint Foundation 2010 (the external IP address for VM2 is 206.130.148.40
- VM 3 (SCFSMO) – Windows 2008 R2 Enterprise (x64), DNS, Active Directory
- VM 4 (3PL) – Windows 2008 R2 Enterprise (x64), Microsoft Dynamics NAV

In addition, all VMs except VM 4 (3PL) are joined to a single internal domain (SCGSC.COM) and all VMs are running Symantec Protection Suite Enterprise 2015.

SCG Secure Cloud has four switches—Cisco 2960 Manageable Switch, Netgear FS524S Unmanaged Switch, Netgear GS108 Unmanaged Switch, and Cisco SG110D-08 Unmanaged Switch. There is one firewall—Cisco 5512-X. External to the SCGSC are two tape backup devices—Tandberg StorageLoader LTO-6 Tape Autoloader with LTO Ultrium and SAS-2 running BackupExec 2015 Enterprise and Tandberg StorageLoader LTO-4

Tape Autoloader. These 2 devices are attached to 2 separate physical servers to perform backup jobs.

Access to the SCGSC System is controlled by the firewall. Access by the public is limited to only http and https to the webserver's application network in the DMZ2. All other traffic is blocked.

Access to manage the SCGSC System is done by manually enabling/disabling access rules to the management network allowing applications tools to make changes.

Production Environment

The production environment is made up of four virtual machines: VM 1 (SCSQL-PROD), VM 2 (SCCOLDSHARE-PROD), VM 3 (SCFSMO), and VM 4 (3PL). The server configuration is listed in Appendix A. This environment is designed to have limited access to and from the public. Incoming traffic (http and https) is only allowed to the webserver (SCCOLDSHARE-PROD). Everything else is blocked by the firewall.

Management of the SCGSC is done manually by allowing management tools (e.g., MS Visual Studio, MS SQL Studio Management, Remote Desktop Sharing, and SMB) to connect to the Management Network. When the management task is completed, these access rules are turned off.

Test Environment

Testing is performed in SCG's development environment.

Development Environment

SCG's development environment is on a separate network from the SCG Secure Cloud and is considered out of the scope of this document.

4.4.2 Solution Infrastructure

The SCG Secure Cloud system is housed in a secure office building in Gaithersburg, MD. The system is located on the 7th floor of the building. There is employee-specific fob-controlled access to SCG's office space, and the SCGSC is located in an employee-specific fob-controlled server room with electronic security that logs the name of each individual entering the room and the date and time of access.

All users are required to be authenticated with user ID and password before access is granted to the system. Additionally, computers used to access the system have to be authorized and be added to the firewall rules to allow access. These computers are required to have up-to-date antivirus software and definitions.

Virtualization Hardware

The virtualization hardware for the SCGSC are the two HP Proliant DL 360 Gen9, which is depicted in the rack in Figure 7. The resource requirements for the production and FAT/UAT/QA environments are listed in Table 6.

Figure 7. Physical Deployed Architecture

Table 6. Resource Requirements for Production and FAT/UAT/QA Environments

Equipment Name	Equipment	Type	Function	Software/ Version
VHOST1	HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, RAID 5	Hardware	Server	VMware VSphere ESXi 6.0 update 2
VHOST1	HP ProLiant DL360 Gen9 – Xeon E5-2620V3 2.4 GHz, 80 GB RAM, 900 GB HD, RAID 5	Hardware	Server	VMware VSphere ESXi 6.0 update 2
SCGSCSW01	Cisco 2960 Manageable Switch Mode3l: WS-C2960-48TC-L	Hardware	Routes traffic to non-privileged user network (internet to apps)	C2960-LAN BASE K9 15.0.2SE7
Unmanaged Switch	Netgear FS524S Unmanaged Switch	Hardware	Routes traffic to management network	NA
SCGSCFW02	Cisco ASA 5512-X Model: ASA 5512v3	Hardware	Filters traffic and maps internal network to external	Cisco Firewall ASA 9.1.2
SCNAS01	HPE 1450 NAS	Hardware	Host Virtual Machines (VMs)	Windows Storage Server 2012 R2
IPS	Added module for Cisco ASA 5512-X Model: ASA 5512v3	Hardware/ Software	Continuously prevents intrusion, Trojans, and hackers	
SCGSCRACK CONV	Startech LCD Serial #: E071X4A40184	Hardware	Display, keyboard, mouse	NA
SCGSCSW03 (Unmanaged Switch)	Netgear GS108 8-Port Gigabyte Switch Serial #: 1DR16B3Y0024E	Hardware	Routes traffic to the DMZ2 network	NA
SCGSCSW04 (Unmanaged Switch)	Cisco SG110D-08 8-Port Gigabyte Switch Serial #: DNI20120CF0	Hardware	iSCSI connection from hosts to NAS device	NA

Load Balancers

The load balancers are the two hosts. These two host are configured to use high availability which behaves like load balancers.

Network Router

There is no router. The Internet Service Provider only provided an ethernet connect for the firewall.

Firewalls

SCGSC has a Cisco ASA 5512-X with IPS. It is connected directly to SCGSC and the corporate firewall.

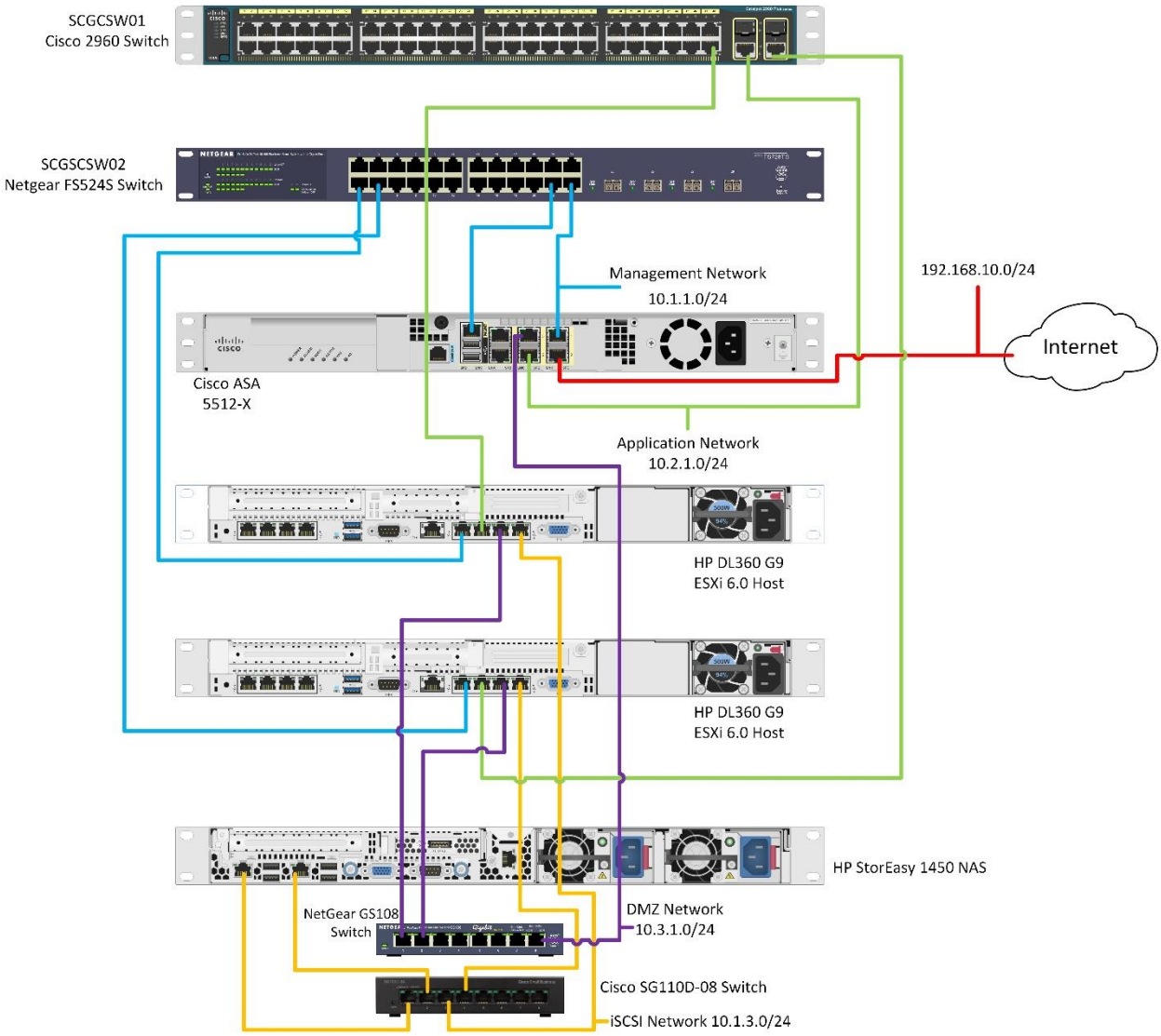
Storage Area Network (SAN)/Network Attached Storage (NAS)

SCGSC has a 4TB HPE 1450 NAS to storage all the virtual machines.

4.4.3 Solution Networking

The SCGSC networking is depicted in Figure 8.

Figure 8. SCGSC Networking Solution



The SCGSC directly addresses the FISMA security controls for boundary protection (SC-7(4)) by:

- Establishing a traffic flow policy for each managed interface;
- Protecting the confidentiality and integrity of the information being transmitted across each interface;
- Documenting each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
- Reviewing exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need.

There are no telecommunication services in the SCGSC system for external telecommunication. All data exchanges are configured to be done securely using http (80) and https (443) (NAT one to one) to web server. The SCGSC isolates a secure network enclave where all systems operate. The open ports for accessing this secure network enclave are identified in Table 7.

Table 7. Open Ports for Accessing the SCGSC Network Enclave

Port (s)	Controls
80 and 443	Access to websites
1433, 1434	Managing SQL database (controlled On/Off manually)
445	SMB – filesharing (controlled On/Off manually)
3389	Remote Desktop Sharing (controlled On/Off manually)
135, 4018, 4019, 4500, 500	Visual Studio (controlled On/Off manually)
80, 443, 902, 5989, 31031, 44046	VSphere management (controlled On/Off manually)
8014	Symantec Endpoint Protection Suite Enterprise communication
25	SMTP – email alerts (one direction from SCGSQL-PROD to corporate Exchange)
53, 88, 123, 135, 137, 138, 139, 389 445 464, 1029, 3268, 3269, 49152-65535	Active Directory
123	NTP (Network Time Protocol)
7046, 7047	MS Dynamics NAV
21, 80, 88, 135, 137, 138, 139, 443, 445, 1125, 1434, 3106, 3527, 6101, 6102, 6103, 6106, 10000	Symantec BackupExec

Of the above listed ports, only 80 and 443 are supported for Public routing interfaces. The remainder of the ports are strictly controlled to the Management Network (See Figure 1) from specifically identified machines using a white list IP Address assignment and security control groups that are managed by Active Directory.

Policies and technical configurations are reviewed quarterly by the IT Director. New policies are established as the demand for them is identified, and they are approved by the System Owner.

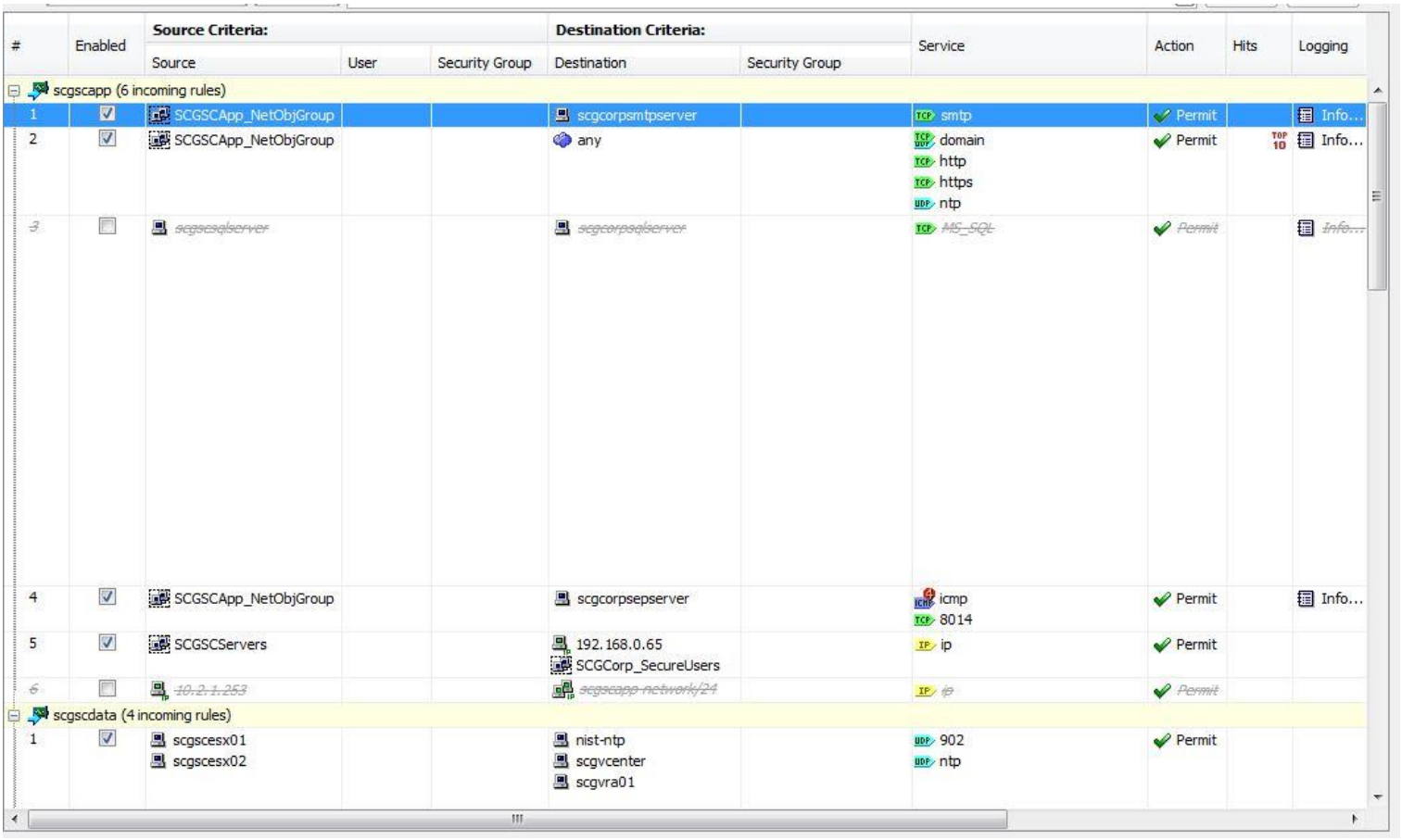
An external and independent assessment team is used to validate appropriate configurations to be in place to meet all FISMA requirements, with annual assessments conducted.

The Cisco firewall IPS and Symantec Endpoint Protection Suite Enterprise protect against or limit the effects of the following types of denial of service attacks: DoS attacks (buffer overflow, ping of death, smurf attack, TCP SYN attack, and teardrop), distributed DoS attacks, amplification attacks, UDP attacks, including volume-based DDoS and application DDoS.

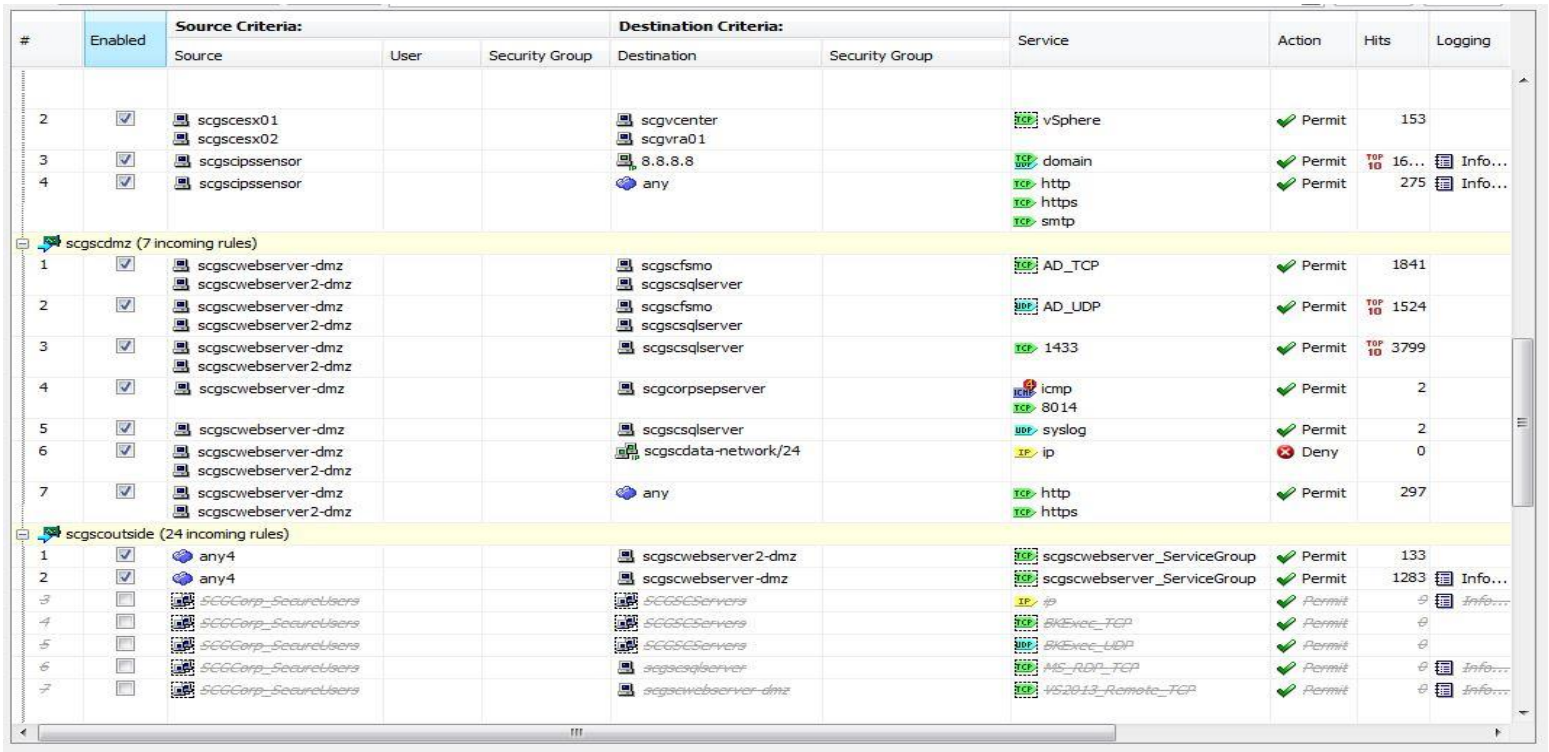
Stateful Packet Inspection (SPI) and IPS are in use at the edge router/firewall. Internal Firewall OS options to prevent DoS are configured such as limited packet fragmentation, Unicast Reverse-Path Forwarding, and DHCP is disabled.

The firewall access rules that are implemented for the SCGSC solution are identified in Figure 9.

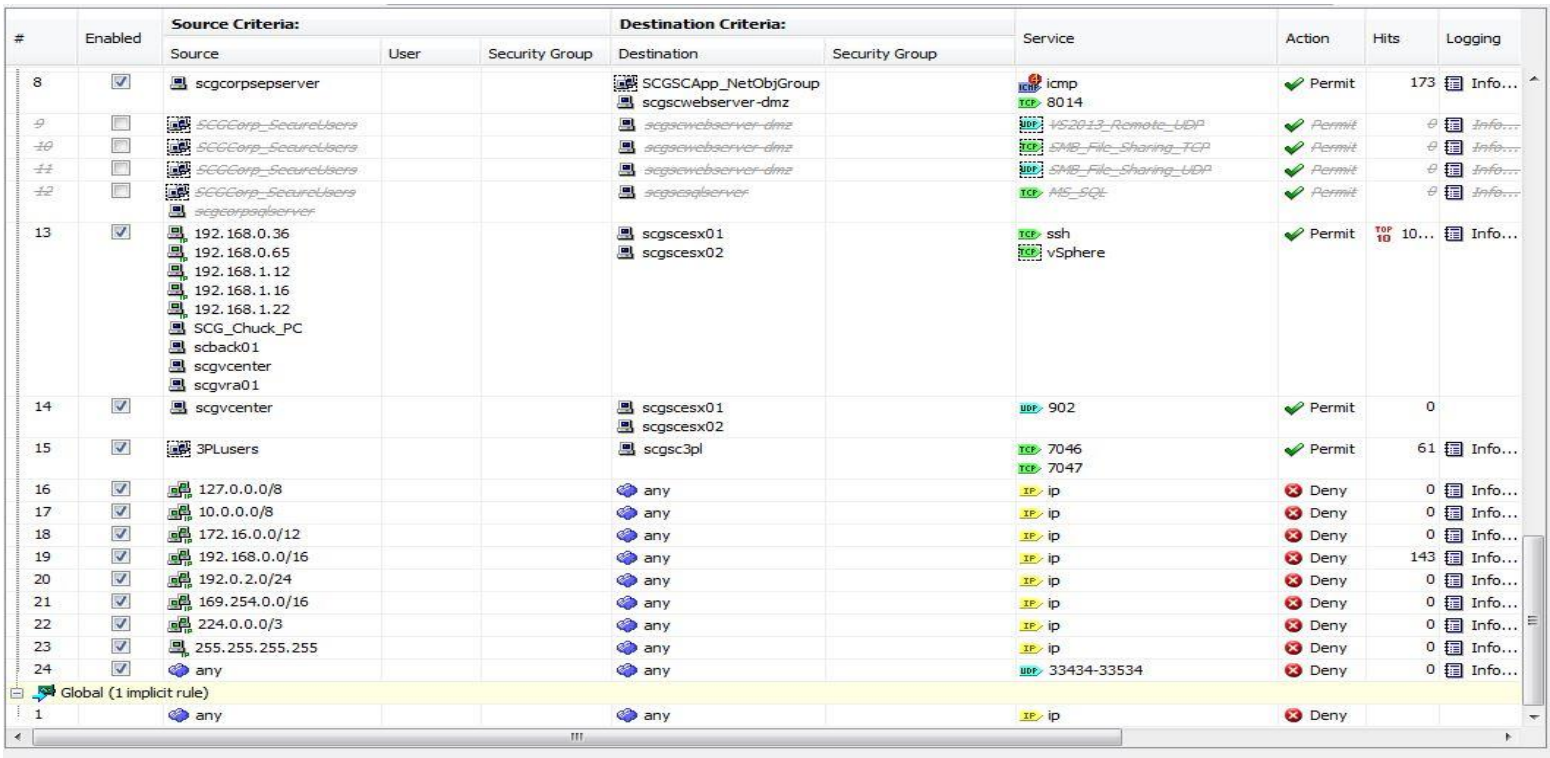
Figure 9. SCGSC Firewall Access Rules



#	Enabled	Source Criteria: Source	User	Security Group	Destination Criteria: Destination	Security Group	Service	Action	Hits	Logging
scgscapp (6 incoming rules)										
1	☑	SCGSCApp_NetObjGroup			scgcorpsmtpserver		smtp	Permit		Info...
2	☑	SCGSCApp_NetObjGroup			any		domain http https ntp	Permit		Info...
~~3~~	☐	~~scgscsqlserver~~			~~scgcorpsqlserver~~		~~MS_SQL~~	~~Permit~~		~~Info...~~
4	☑	SCGSCApp_NetObjGroup			scgcorpsepserver		icmp 8014	Permit		Info...
5	☑	SCGSCServers			192.168.0.65 SCGCorp_SecureUsers		ip	Permit		
~~6~~	☐	~~10.2.1.253~~			~~scgscapp-network/24~~		~~ip~~	~~Permit~~		
scgscdata (4 incoming rules)										
1	☑	scgscesx01 scgscesx02			nist-ntp scgvcenter scgvra01		902 ntp	Permit		



#	Enabled	Source Criteria: Source	User	Security Group	Destination Criteria: Destination	Security Group	Service	Action	Hits	Logging
2	☑	scgscesx01 scgscesx02			scgvcenter scgvra01		vSphere	Permit	153	
3	☑	scgscipssensor			8.8.8.8		domain	Permit	16...	Info...
4	☑	scgscipssensor			any		http https smtp	Permit	275	Info...
scgscdmz (7 incoming rules)										
1	☑	scgscwebserver-dmz scgscwebserver2-dmz			scgscfsmo scgscsqlserver		AD_TCP	Permit	1841	
2	☑	scgscwebserver-dmz scgscwebserver2-dmz			scgscfsmo scgscsqlserver		AD_UDP	Permit	1524	
3	☑	scgscwebserver-dmz scgscwebserver2-dmz			scgscsqlserver		1433	Permit	3799	
4	☑	scgscwebserver-dmz			scgcorpsepserver		icmp 8014	Permit	2	
5	☑	scgscwebserver-dmz			scgscsqlserver		syslog	Permit	2	
6	☑	scgscwebserver-dmz scgscwebserver2-dmz			scgscdata-network/24		ip	Deny	0	
7	☑	scgscwebserver-dmz scgscwebserver2-dmz			any		http https	Permit	297	
scgscoutside (24 incoming rules)										
1	☑	any4			scgscwebserver2-dmz		scgscwebserver_ServiceGroup	Permit	133	
2	☑	any4			scgscwebserver-dmz		scgscwebserver_ServiceGroup	Permit	1283	Info...
~~3~~	☐	~~SCGCorp_SecureUsers~~			~~SCGSCServers~~		~~ip~~	~~Permit~~	~~0~~	~~Info...~~
~~4~~	☐	~~SCGCorp_SecureUsers~~			~~SCGSCServers~~		~~BKExec_TCP~~	~~Permit~~	~~0~~	
~~5~~	☐	~~SCGCorp_SecureUsers~~			~~SCGSCServers~~		~~BKExec_UDP~~	~~Permit~~	~~0~~	
~~6~~	☐	~~SCGCorp_SecureUsers~~			~~scgscsqlserver~~		~~MS_RDP_TCP~~	~~Permit~~	~~0~~	~~Info...~~
~~7~~	☐	~~SCGCorp_SecureUsers~~			~~scgscwebserver-dmz~~		~~VS2013_Remote_TCP~~	~~Permit~~	~~0~~	~~Info...~~



#	Enabled	Source Criteria: Source	User	Security Group	Destination Criteria: Destination	Security Group	Service	Action	Hits	Logging
8	☑	scgcorpsepserver			SCGSCApp_NetObjGroup scgscwebserver-dmz		icmp 8014	Permit	173	Info...
~~9~~	☐	~~SCGCorp_SecureUsers~~			~~scgscwebserver-dmz~~		~~VS2013_Remote_UDP~~	~~Permit~~	~~0~~	~~Info...~~
~~10~~	☐	~~SCGCorp_SecureUsers~~			~~scgscwebserver-dmz~~		~~SMB_File_Sharing_TCP~~	~~Permit~~	~~0~~	~~Info...~~
~~11~~	☐	~~SCGCorp_SecureUsers~~			~~scgscwebserver-dmz~~		~~SMB_File_Sharing_UDP~~	~~Permit~~	~~0~~	~~Info...~~
~~12~~	☐	~~SCGCorp_SecureUsers~~ ~~scgcorpsqlserver~~			~~scgscsqlserver~~		~~MS_SQL~~	~~Permit~~	~~0~~	~~Info...~~
13	☑	192.168.0.36 192.168.0.65 192.168.1.12 192.168.1.16 192.168.1.22 SCG_Chuck_PC scback01 scgvcenter scgvra01			scgscesx01 scgscesx02		ssh vSphere	Permit	10...	Info...
14	☑	scgvcenter			scgscesx01 scgscesx02		902	Permit	0	
15	☑	3PLusers			scgsc3pl		7046 7047	Permit	61	Info...
16	☑	127.0.0.0/8			any		ip	Deny	0	Info...
17	☑	10.0.0.0/8			any		ip	Deny	0	Info...
18	☑	172.16.0.0/12			any		ip	Deny	0	Info...
19	☑	192.168.0.0/16			any		ip	Deny	143	Info...
20	☑	192.0.2.0/24			any		ip	Deny	0	Info...
21	☑	169.254.0.0/16			any		ip	Deny	0	Info...
22	☑	224.0.0.0/3			any		ip	Deny	0	Info...
23	☑	255.255.255.255			any		ip	Deny	0	Info...
24	☑	any			any		33434-33534	Deny	0	Info...
Global (1 implicit rule)										
1		any			any		ip	Deny		

4.4.4 Storage and Backup Solution

The SCGSC has 4TB of storage. All data are backed up onto LTO-6 tapes using Symantec BackupExec 2015 from primary and alternate sites.

The SQL Server is configured to provide warning notifications when approaching the limits of storage capacity.

4.4.5 Security Architecture

The SCGSC system makes use of specific enterprise system and security services, which comprise major elements of the security architecture. Some of these features include:

- The SCGSC utilizes Symantec EndPoint Protection Suite Enterprise 2015 as a COTS based solutions for antivirus, malware, and code execution (runtime memory) protection.
- The SCGSC utilizes Windows Embedded Security features to protect against unauthorized code or application execution. Specifically, Windows Server 2008 R2 is configured to enforce User Access Control (UAC). UAC monitors the authorized and trusted applications that are available within the Windows Operating System (OS), and will automatically block the execution of any code, program, or application that is not manually granted access to run in the runtime memory or execute as an authorized system process on the OS platform.
- The SCGSC also utilizes the Windows Kerberos security services for authentication and authorization services. Users are expected to provide credentials, which are a User ID and password, for identification and authentication to access the Server. These credentials are converted into a secure hash and presented to the Kerberos security engine for validation. Upon successful hash comparison, the Windows Kerberos service establishes a “Ticket” that is presented to trusted and authorized applications and services that are resident or accessible to the Windows platform. This “Ticket” serves as a one-time login credential that will allow for the execution of code at runtime, the initiation of an application and a related session, or the ability to engage Windows Services that are authorized for that identified user.
    - Authentication to the SCG Secure Cloud does not support persistent session, which removes any capability to support replay attacks to the environment. The environment utilizes Microsoft Authentication capabilities that leverage Kerberos services. Utilization of this authentication framework allows for ticket granting services that resist replay attacks to the environment. Additional security can be configured when the business or technical demands are identified for this solution.
- Windows Security services also provide the SCGSC an environment that operates as Least Privilege. The group membership configured within Active Directory or at the Local Administrative level enforces least privilege in accordance with Microsoft best practices.
- Each of the servers within the SCGSC have been appropriately reviewed to implement high security configurations for web and data management services. The manner with which SCGSC supports each hosted application allows for an

appropriate separation of security and protects against data access from unauthorized sources or persons:

  - Windows IIS configurations have been appropriately secured, whereby each Application Pool is separate and distinct for any hosted applications. This effectively segregates the security function that is subject to the security protections and boundary of any hosted application in the SCGSC.
  - SQL Database configures utilize an independent data blob to support each hosted application within the shared data storage environment. Independent database level accounts and security controls are configured at the direction of the hosted application, appropriately engaging the security architecture and configuration of the individual application and its corresponding database.

- The SCGSC does not, in of itself, store any user or application data. The SCGSC provides the infrastructure level services that allow for the execution of code, application processes, and system actions for the hosted applications. The only data collected by the SCGSC is data related to audit processes and security processes that are within the scope of the solution architecture, which is inclusive of only the Windows Servers and the VMware ESXi hosts. SQL databases are manually purged every 30 days.
  - Audit logs are retained for a period of three years in full compliance with SCG organizational policy. Additional long term solutions can be implemented when a requirement is identified by the government to do so.
- The SCG Secure Cloud local user accounts only permit access to the hosting platforms for applications and systems (e.g., Windows logon). Access is not transferable to hosted applications. Each individual application that is hosted in the SCG Secure Cloud maintains its own respective access control as defined by the application owner. In addition, the current set of Firewall rules are set to isolate communications from Applications and Data tiers established in the secure network enclave.
- All hosting platforms in the SCG Secure Cloud are configured to not permit Remote Desktop (RDP) to Windows servers.
- vSphere connections are permitted to allow access to ESX hosts, but only from specific workstations. These connections are directly permitted via edge router/firewall rules to allow for appropriate protection mechanisms for accessing the hosting environment.
- A “banner” is in place for any log in events to the ESX host and Windows systems.
- Non-privilege or GUEST accounts are not supported by any component of the system
- The Windows OS Event Log provides a record of all accesses or attempts for access to the system. This log data is aggregated by the Kiwi Syslog application/service.
- Password management is configured in full alignment with FISMA requirements, which includes:

  - Minimum password lengths are configured into each local machine policy for the Windows OS environment and they exceed these control requirements.
  - Minimum password lengths are configured into each local machine policy for the Windows OS environment and they exceed these control requirements.
  - A hash is used instead of the password which meets this control.
  - Minimum password lengths are configured into each local machine policy for the Windows OS environment and they exceed these control requirements.
  - Passwords cannot be reused as a function of the local machine policy configured at each Windows OS environment.
  - Temporary passwords are not supported per organizational policy.
- User access is strictly controlled and enforced in the following way:
  - Users are provided an account by the IT Director. The accounts are known only to the IT Director and the individual and an in-person exchange of information is done to provide the user an account.
  - Authenticators adhere to policies that are implemented within the individual hosting platforms that comprise the SCG Secure Cloud solution.
  - The password rules are established in the Windows Local Policy settings and are enforced by this COTS solution.
  - The SCG IT Director personally manages these processes with in person validation of identity and ensures that authenticators adhere to organizational policy.
  - The default passwords for the SCG Secure Cloud solution have all been changed post installation.
  - The Windows Local Machine Policies establish the rules for a maximum of 90 days for password longevity
  - The SCG Secure Cloud solution utilized a Windows based mechanism for password change that is secure and enforceable through Local Machine policies.
  - Passwords are known only to the account holder and are encrypted by Microsoft to keep them from being discovered. The passwords are presented as a hash to the Operating System utilizing a symmetric key exchange style of approach, which adequately protect from password discovery.
  - This is not applicable as the authenticator (password) remains encrypted and only a secure hash is exchanged with the MS Kerberos services.
  - Users are all stored in a single group and membership changes are not applicable to this solution.

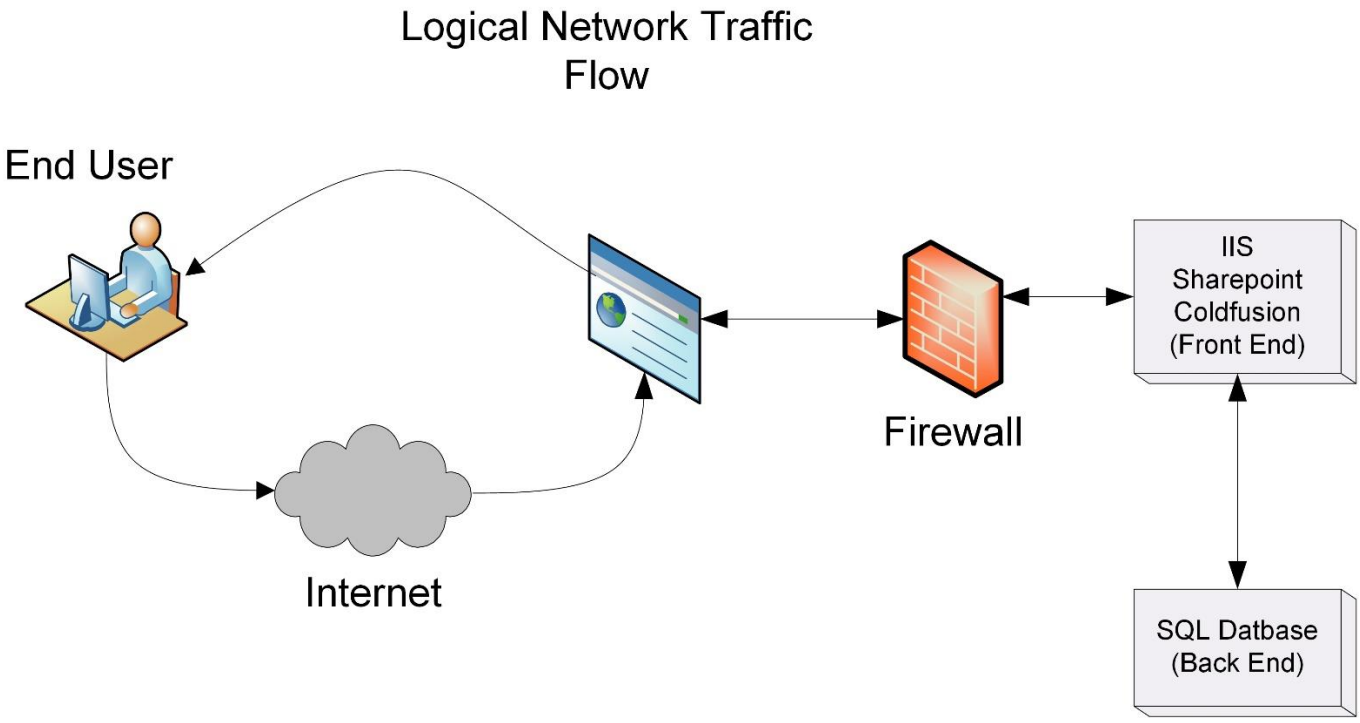
Note: *SCGSC Domain passwords stored by the system are protected using reverse encryption. Stored passwords for the SCGSC firewall also are encrypted.*

5. System Interfaces

This section discusses and describes the system interfaces that exist between the SCGSC and external systems.

Figure 10 shows how the user interfaces with the SCGSC system.

Figure 10. User Interfaces with the SCGSC System



Users can access the SCGSC from publically routable sources (e.g., Internet). The users can access applications through their defined User Interfaces, in a manner that is permissible and supported by each independent application and using the credentials and application security models that are configured within each independent application. The user does not interact directly with the SCGSC system, but only interacts with the applications that are hosted within the SCGSC system/solution.

Any supported application that is configured to utilize data storage (data tier) capabilities is permitted the access needed for such access. Data read and write operations are controlled by the hosted application directly, and no direct data read/write activities are supported through circumvention of the configured application User Interface.

Select users with administrative or specially configured privileges may have the ability to interface directly with the SQL database of the websites. These users are subject to the specific security models and architectures that are pre-configured into the hosted applications. Each database that is linked to a hosted application is provided by the government with its own security controls, and these are outside of the scope of control of the SCGSC.

SGC Administrative users are preconfigured into security roles and granted special access rights to SGCSC systems, servers, and applications. These users originate an interface from a White Listed machine from the SCG Corporate Network, which is appropriately controlled by configurations resident in the SCGSC Firewall. The Access Control Lists, group memberships, and related Role/Rule Based access control component are

configured within the SCGSC target application or platforms. A challenge response mechanism is engaged to appropriate Identify, Authenticate, and Authorize the Administrative users' access to the target platform.

Interactions with the underlying hosting services that are provided by the SCGSC do not have a direct impact on the security or configurations of the hosted applications or services provided by NIDDK. The Administrative users are limited in function to maintaining and operating the hosting services that are offered as the SCGSC core function.

Table 8 provides details on how users interface with the SCGSC system.

Table 8. User Interfaces with SCGSC

Step	Details
Internet user initiates request	User enters front end of website using internet protocol http (80) or https (443). This happens in the DMZ2 (Application network).
System accesses database	Back-end of system contacts SQL server and reads/writes to the database
Information is received by user	Information is sent to user

5.1.1 Application Partitioning

The SCGSC separates user functionality (including user interface services) from information system management functionality and this enforced through the firewall rules.

5.1.2 Information in Shared Resources

The SCGSC system prevents unauthorized and unintended information transfer via shared system resources by controlling user level access to resources.

Appendix A: Server Configurations

A. Server Configurations – Development Environment

Server name: SCCOLDSHARE-DEV

OS: Windows 2008 R2 Enterprise 64Bit with SP1

WORKGROUP: WORKGROUP

Hard drive partition: Single logical drive (C: Drive)

Hard format: NTFS

Hard drive size: 300 GB

RAM: 8 GB

Processor: 2

B. Server Configurations – Test Environment

Testing is done in the development environment.

C. Server Configurations – Production Environment

Server name: SCCOLDSHARE-PROD

OS: Windows 2008 R2 Enterprise 64Bit with SP1

Domain: SCGSC.COM

Hard drive partition: Single logical drive (C: Drive)

Hard format: NTFS

Hard drive size: 500 GB

RAM: 16 GB

Processor: 4

Software Installed:

- IIS 7.0
- Coldfusion 9
- Sharepoint Foundation 2010 (64Bit)
- Symantec Endpoint Protection Suite Enterprise 2015

Server name: SCSQL-PROD

OS: Windows 2008 R2 Enterprise 64Bit with SP1

Domain: SCGSC.COM

Hard drive partition: Single logical drive (C: Drive)

Hard format: NTFS

Hard drive size: 250 GB

RAM: 16 GB

Processor: 4

Software Installed:

- MS SQL 2012
- Kiwi Syslog 9.4.1
- Symantec Endpoint Protection Suite Enterprise 2015
- DNS Server (secondary)

Server name: SCFSMO

OS: Windows 2008 R2 Enterprise 64Bit with SP1

Domain: SCGSC.COM

Hard drive partition: Single logical drive (C: Drive)

Hard format: NTFS

Hard drive size: 100 GB

RAM: 8 GB

Processor: 2

Software Installed:

- Symantec Endpoint Protection Suite Enterprise 2015
- DNS Server (primary)
- Active Directory

Server name: 3PL

OS: Windows 2008 R2 Enterprise 64Bit with SP1

Domain:

Hard drive partition: Two logical drives (C: and E: Drives)

Hard format: NTFS

Hard drive size C: 200 GB

Hard drive size E: 350 GB

RAM: 8 GB

Processor: 4

Software Installed:

- MS Dynamics NAV
- Symantec Endpoint Protection Suite Enterprise 2015