POL00398165

Document Title: Network Security High Level Design

Document Reference: DES/NET/HLD/0016

Document Type: High Level Design (HLD)

Release: Not Applicable

Abstract: Provides a High Level overview of the network security components and appliances and positioning required to secure the HNG-X solution.

Document Status: DRAFT

Author & Dept: Sean Kerrin

External Distribution:

Approval Authorities:

Name	Role	Signature	Date
Steve Dingle	Solution Design		
Graham Allen	HNG-X Development		

Note: See Royal Mail Group Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

POL00398165

0 Document Control

0.1 Table of Contents

POL00398165

POL00398165

POL00398165

0.2 List of Figures

0.3 List of Tables

POL00398165

0.4 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	11-Jul-07	First Draft	
0.2	6-Aug-07	Rewrite of document and creation of Second Draft after Receiving Guidance on Document Scope	

0.5 Review Details

Review Comments by :	Monday 17th September 2007
Review Comments to :	sean.kerrin GRO & RMGADocumentManagement GRO
Mandatory Review	
Customer Solution Architect	Dave Haywood
Network Designer	Temitayo Fashina
Network Designer	Stephen Wisedale
Network Designer	Rahman El-Khoulali
Development	Graham Allen
SCC	Mik Peach
Business Continuity	Tony Wicks
System Test	Harjinder Hothi
Security Architect	Jim Sweeting
Network Architect	Mark Jarosz
Migration Architect	Jeremy Worrell
Business Continuity	Tony Wicks
Security	Bill Membery
Optional Review	
Network Designer	Ghalib Al-Kilidar
Customer Solution Architect	Ian Devereux
ZenSar Design Lead	Gautam Das
Programme Manager	Phil Day
Applications Architecture	Dave Johns
Test Design	Peter Robinson
Test Design	George Zolkiewka
Head of Service Management	Steve Denham
Head of Service Change & Transition	Graham Welsh
HNG-X Service Transition	Steve Godson
Service Support	Peter Thompson

POL00398165

Service Network	Alex Kemp
Data Centre Migration	Martin Brett
Infrastructure Design / Solution Design	David Sackman / Steve Dingle
Integration	David Hinde
Testing	Peter Dreweatt
SV&I Manager	Sheila Bamber
Tester	Hamish Munro
RV Manager	James Brett (POL)
VI Manager	Peter Rickson
TE Manager	Peter Rickson
HNG-X Acceptance & Risk	Wayne Roberts (POL)
Core Services	Pat Lywood
Core Services	Ed Ashford
Core Services	Andrew Gibson
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name
Project Manager	Dean Parsons

(*) = Reviewers that returned comments

0.6 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	2.0	16-Apr-07	(Document Title)	Dimensions
ARC/NET/ARC/0001	V0.4	8/5/07	HNG-X Technical Network Architecture	Dimensions
ARC/SEC/ARC/0003	V1.0	16/2/07	HNG-X Technical Security Architecture	Dimensions
DES/NET/HLD/0008	V0.2	4/6/07	Data Centre LAN Design	Dimensions
DES/NET/HLD/0009	V1.0	9/8/07	HNG-X Wide Area Network HLD	Dimensions
DES/NET/HLD/0014	V0.1	20/7/07	HNG-X Branch Access Network HLD	Dimensions
DES/NET/HLD/0010	V0.4	5/7/07	Branch Router Network HLD	Dimensions
DES/NET/HLD/005	V0.2	2/3/07	HNG-X Data Centre Network Security HLD	Dimensions

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

POL00398165

0.7 Abbreviations

Abbreviation	Definition
AAA	Authentication, Authorisation and Accounting
ACE	Application Control Engine
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ASDM	Adaptive Security Device Manager
AUX	Auxillary
BCP	Best Current Practice
BGP	Border Gateway Protocol
BT	British Telecommunications PLC
BTL01	Bootle data centre
CE	Customer Edge
CEF	Cisco Express Forwarding
CoPP	COntrol Pane Policing control
CoS	Class Of Service (IEEE802.1p) (layer 2 QoS)
DAI	Dynamic ARP Inspection
dCEF	Distributed Cisco Express Forwarding
DMS	Degrees, Minutes, Seconds
DWDM	Dense Wave Division Multiplexing
DMZ	De-Militarised Zone
DRS	Data Reconciliation Service
DTP	Dynamic Trunking Protocol
DWH	Data WareHouse
FWSM	Firewall Services Module
GMT	Greenwich Mean Time
HP	Hewlett Packard
IDS	Intrusion Detection System
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IRE11	Ireland 11 data centre
IRE19	Ireland 19 data centre
ITU	Infrastructure Test Unit
LAN	Local Area Network
MSFC	Multi-layer Switch Feature Card
NNM	Network Node Manager

POL00398165

Abbreviation	Definition
NPS	Network Persistence Store
NTP	Network Time Protocol
OEE	Overall Equipment Effectiveness
OS	Operating System
OSPF	Open Shortest Path First
OVO	OpenView Operations
PDU	Power Distribution Unit
PFC	Policy Feature Card
POA	Post Office Account
PVST+	Per-VLAN Spanning Tree +
QoS	Quality Of Service
RFC	Request For Comments
RMGA	Royal Mail Group Account
SAN	Storage Area Network
SIN	Suppliers' Information Note
STD	Standard
TES	Transaction Enquiry Service
TPS	Transaction Processing System
TTY	Teletype
UDLD	Uni-Directional Link Detection
UPS	Uninterruptible Power Supply
UTC	Coordinated Universal Time
VLAN	Virtual LAN
VLSM	Variable Length Subnet Mask
VRF	Virtual Routing & Forwarding
VRRP	Virtual Router Redundancy Protocol (RFC3768)
VTP	VLAN Trunking Protocol (IEEE802.1q)
VTY	Virtual Teletype
WAN	Wide Area Network
WGN01	Wigan data centre

0.8 Glossary

Term	Definition
AAA	AAA is Cisco's framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

POL00398165

Term	Definition
DMZ	A DMZ is a subnet between a trusted internal network and an untrusted external network. Typically, the DMZ contains publicly accessible systems (e.g., Web servers, file servers, mail servers and DNS servers). It usually is located at the perimeter of the trusted internal network.
DWDM	Dense Wave Division Multiplexing. A technique for multiplexing many data streams (usually 32) over a single fibre optic cable by using different frequency laser optics.
Production	When referring to data centre use, indicates the data centre primarily providing service to the customer business. Normally the Primary data centre at IRE11.
Test	When referring to data centre use, indicates the data centre primarily providing a test service. Normally the Secondary data centre in IRE19.

0.9 Changes Expected

Changes
Addition of further information on IDS/IPS and CSM tool.

0.10 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.11 Copyright

POL00398165

1 Introduction

This is the Network Security High Level Design that supports the parent documents found within Dimensions, namely HNG-X Technical Network Architecture ARC/NET/ARC/0001 and HNG-X Technical Security Architecture ARC/SEC/ARC/0003.

1.1 Purpose

The purpose of this document is to provide a high level description/overview of the network security components and appliances and considers the positioning required to secure the HNG-X solution. It is designed to expand on the security elements of the solution that have been identified within the Technical Network Architecture and Technical Security Architecture documents.

1.2 Readership

This document should be reviewed by those within the design, implementation and support group who may have a specific interest in the security aspects of the HNG-X solution.

1.3 Scope

This document maps out the High Level strategy and requirements for implementing security into the HNG-X design. It concentrates primarily on the following areas:

- Network Security Policy
- Network Tiers
- DMZ's
- Network Attacks
- Network Security features
- Firewalls
- Network Controls in General

1.4 Assumptions

It is assumed that workshops will be held:

- To determine the control and rule set of security devices such as firewalls, IPS and ACL controlled routers.
- To examine and understand server and application traffic flows

1.5 Risks

- Internal risk is that lack of workshops will prevent LLDs from being created

POL00398165

1.6 Dependencies

Knowledge of system traffic flows and server communication is required prior to determining the firewall and IPS/IDS rule sets.

A level of understanding is needed about server platforms and their positioning and purpose in the network as determined by the system architecture.

1.7 Constraints (Standards, Policies, Guidelines)

The design must conform to the architecture and policy set out in the parent documents

- HNG-X Technical Network Architecture ARC/NET/ARC/0001
- HNG-X Technical Security Architecture ARC/SEC/ARC/0003

1.8 Principles

As stated within the HNG-X Technical Security Architecture the following specific principles provide the foundation for this Network Security High Level Design

- Control access to, from and within the HNG-X infrastructure
- Ensure anomalous activity is detected and responded to
- Least privilege i.e
    - Restrict access using the principle of ”that which is not explicitly granted is denied” or a “default deny” stance
    - Traffic passing between security domains must be controlled to only allow the relevant protocol and port necessary for the service being accessed.
- Defence in Depth
    - Use a layered approach to security to provide multiple controls for prevention and detection
- Secure defaults
    - All default settings , particularly passwords and SNMP communities must be changed before LIVE deployment
- Check at the Gate
    - Check access as early as possible. Detect and prevent unauthorised access as early as possible.

2 Requirements Tracking

The following requirements should be met as part of the Network Security design i.e those areas that are concerned with the network security rather than business requirements

Ref:	Description
SEC-3133	All new developments will protect databases from SQL injection attacks mounted through data centre perimeter controls such as firewalls.

POL00398165

Ref:	Description
SEC-3140	No password shall be transmitted in clear text across any network, whether internal or external.
SEC-3156	{CISP 8.5.1c} Controls shall protect against denial-of-service attacks originating from non-Horizon systems including those listed in Requirement SEC-3152.
SEC-3160	All HNG-X systems shall use private IP addresses which shall not be exposed across the system boundary.
SEC-3162	{CISP 8.5.1e} Network management staff within each domain shall be alerted to any attempt to reach the HNG-X systems in their domain from unauthorised network addresses.
SEC-3165	Individual attempts to breach network security controls shall be treated as a minor security breach. A concerted attempt or a successful breach of network security controls shall be treated as a major security breach.
SEC-3167	{CISP 8.5.1g} Data over Wide Area Networks shall be encrypted unless specifically agreed in the relevant Technical Interface Specification or where otherwise specifically agreed by Post Office Limited Information Security. The Fibre Optic link between Data Centres is not considered to be a Wide Area Network. The requirement applies to transaction data between branches and the data centre(s).
SEC-3168	WAN Encryption key management shall be independent of network configuration such that the confidentiality of Post Office traffic is not compromised by a single configuration error of either the WAN or the encryption system.
SEC-3169	{CISP 8.5.1h} The system design shall require that no encrypted data is to pass through any HNG-X firewall layer other than certain defined fields in the application level protocol (e.g. encrypted PINs) except where data is subsequently decrypted and passes through another firewall layer. Other cases may be authorised by Post Office Information Security where a risk assessment has identified that the requirement for confidentiality outweighs the requirement for system availability and integrity.
SEC-3170	All proposals for encrypted data to pass through any HNG-X firewall layer shall be subject to risk assessment to determine if the requirement for confidentiality outweighs the requirement for system availability and integrity.
SEC-3172	Cases requiring encrypted data to pass through any HNG-X firewall layer shall only be authorised by Post Office where a risk assessment has identified that the requirement for confidentiality outweighs the requirement for system availability and integrity.
SEC-3174	{CISP 8.5.1j} Test systems shall only share logical network connection with operational systems in carefully controlled circumstances. Test systems shall be configured to connect in this manner for the minimum duration necessary to support testing. The logical connection shall only be permitted after an assessment has confirmed that live operation will not be adversely impacted or as otherwise agreed by Post Office Limited.
SEC-3176	All RADIUS servers that authenticate network access shall be secured and segregated into logical network segments by carrier access method and be externally visible to authorised domain users only.
SEC-3204	Such update shall include at least the following password requirements: Minimum password length of 7, Minimum password history length of 4
SEC-3235	All cryptographic key lengths shall be at least 128 bits for symmetric keys and at least 1024 bits for asymmetric keys where the associated cryptographic control protects the integrity or confidentiality of HNG-X Business Data, Reference Data or Application Software unless otherwise agreed with Post Office Information Security. Note: Post Office is highly unlikely to agree to any shorter keys lengths (even for COTS products). For the avoidance of doubt, access to the TES Query service is not covered by this requirement but by requirement SEC-3236.

3 HNG-X Network Overview

POL00398165

HNG-X solution is concerned with providing LAN and WAN services for multiple areas. As a consequence network security must be considered for all areas. An overview of the target network solution is outlined at 3.1

3.1 Target Network Solution

Figure 1 below (taken from ARC/NET/ARC/0001) depicts the network architecture that will be in place. The architectural design already has a layered approach in terms of routing and switching environments, and provides demarcation points that can be used to enforce and manage security policy. However, the requirement for operational traffic to traverse the LANs and WANs introduces a security concern and by definition requires that safeguards are put in place. The central LAN needs to be protected from attacks from any number of possible locations from outside. To provide a suitable layered security solution the architecture can be mapped against a network tier model.

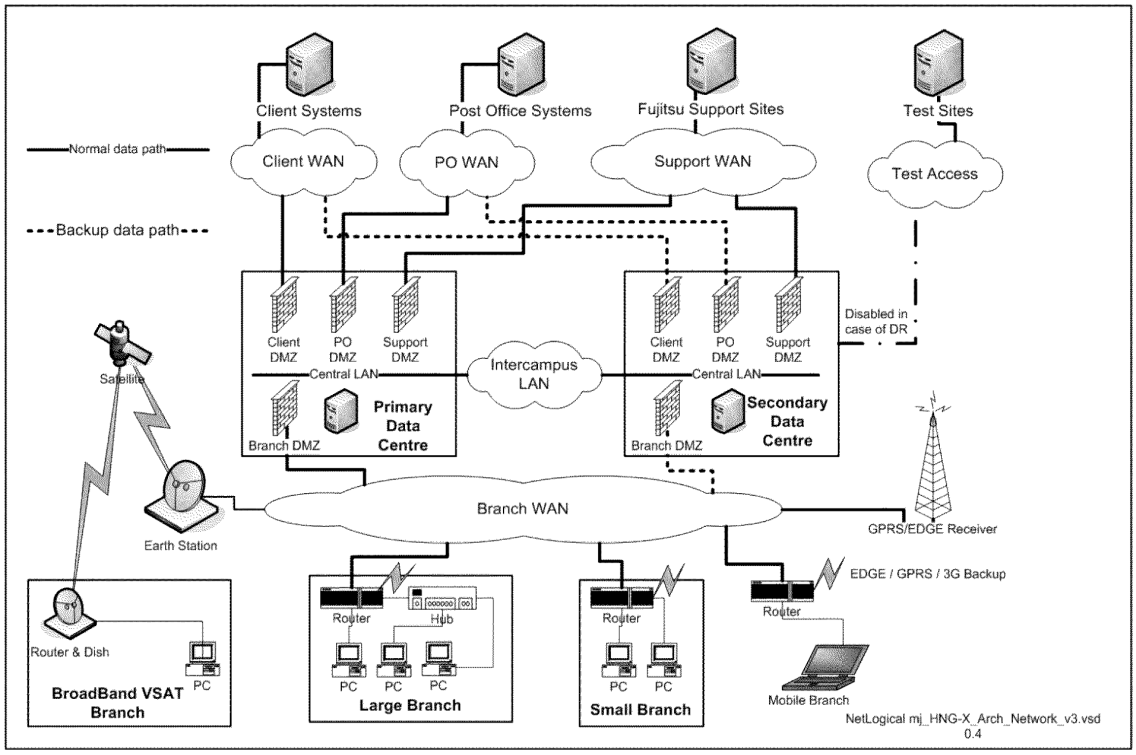

Figure 1 – Overall view of the HNG-X Target Network solution

3.1.1 Network Tier

The three tier model identifies the Access, Distribution and Core Tiers. In doing so it provides a way of separating and isolating the various traffic flows and types needed and can be used as a method of applying the security controls required to protect the network. Figure **2** (taken from ARC/NET/ARC/0001) below highlights the elements of HNG-X solution.

POL00398165

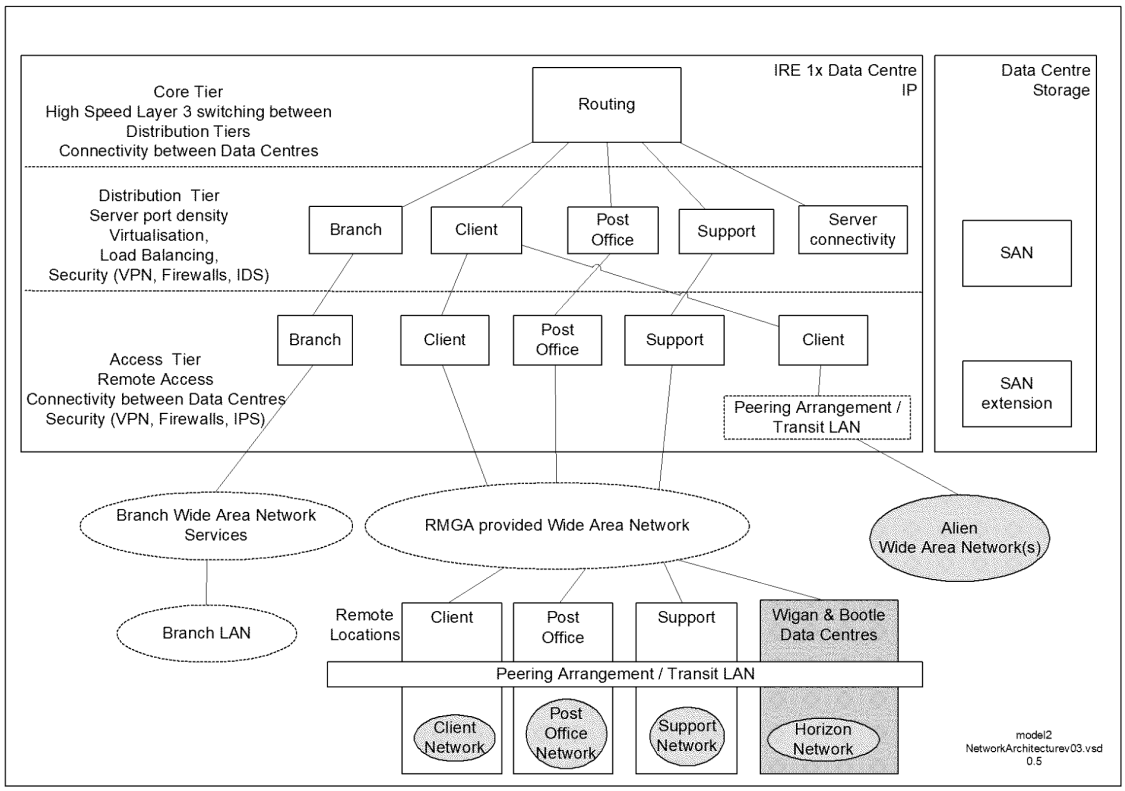

Figure 2 - Network Model

3.1.1.1 Core Tier

This is the environment where high speed layer 3 switching takes place with the emphasis being placed on switching traffic as quickly as possible and providing redundant and fast converging connectivity between the other datacentre and also the areas within the distribution tier. High throughput and optimal routing is the priority within this tier; latency caused by protection mechanisms such as firewalls and ACL's is not wanted. The policy must be that the traffic within this tier has already been inspected and deemed valid.

3.1.1.2 Distribution Tier

This is the layer at which aggregation, routing, server port density, access control and QOS are provided. Load balancing, server virtualisation, policy based connectivity and security are some of the features that are also used. At this tier the security solutions or components that can be expected to be used are firewalls, VPNs, IDS/IPS. For the HNG-X design the Cisco Firewall Services Module (FWSM) blade will be deployed in the Core 6513s.

3.1.1.3 Access Tier

POL00398165

This tier is designed to provide typically workgroup access. In terms of the HNG-X solution the access tier provides remote sites access from across the WAN to the central LANs and HNG-X system housed within the data centres. The HNG-X access tier has network security solution in use and traffic flows are protected with the use of Application Control Engine (ACE) blade in the 6513 for SSL termination from the counters, and an ASA firewall and McAfee IPS component to protect unwanted traffic from the Core 6513. The Access Tier, within the DMZ, has RADIUS platforms to authenticate access from the Branch network.

4 Network Security Design

4.1 Network Security Overview

4.1.1 Security Policy

HNG-X Network Security requires layers of security within the network which will be implemented using the the following steps

- **Securing** the HNG-X Network
- **Monitoring** the HNG-X Network
- **Testing** the HNG-X Network
- **Improving** the HNG-X Network

4.1.1.1 Securing the HNG-X Network

This involves implementing the techniques of filtering, authenticating and encrypting traffic by using both system and network devices. in order to meet the requirements of the security policy.

4.1.1.2 Monitoring the HNG-X Network

System auditing and intrusion detection is required to monitor and detect violations.

4.1.1.3 Testing the HNG-X Network

Regular system auditing and vulnerability scanning will validate the security policy implemented.

4.1.1.4 Improving the HNG-X network

Monitoring and testing the security policy and solution will provide information as to how to improve on the security implementation. Emerging security threats will mean changing the parameters of the HNG-X security policy and to carry out vulnerability patching.

4.1.2 Security Strategy and Solutions

The network security strategy of Prevention, Containment, Detection and Response can be viewed in the following way

- To prevent attack from **outside** the HNG-X infrastructure by ensuring that the perimeter of the network is secured by firewalls and IDS/IPS - SECURING

POL00398165

- To prevent attack from **within** the HNG-X infrastructure by containing and detecting traffic using network segmentation (VLANs), access controls lists (ACLs), firewalls and IDS/IPS - SECURING
- To detect potential violation of network with use of IDS/IPS and firewall logging - MONITORING
- To log and audit activity on each security device to a Management system - TESTING
- To control access to network devices via Identity and Security Management (RADIUS/TACACs) - IMPROVING
- To respond to threats i.e harden the security policies based on log and audit findings

The aims above are achieved by utilising the various security solutions available such as

- Firewall for filtering
- IDS /IPS for detecting violations of policy
- VPN's for securing WAN traffic
- Anomaly Detection and Mitigation for identifying unusual traffic patterns
- Endpoint security for locking down end devices
- Identity and Audit Management i.e. authentication via RADIUS and logging
- Security Management via TACACs for configuration and control of network components

4.2 Security Demarcation Points

The network security policy of protecting the network and system data from any potential threat at the earliest possible moment is to be used with regards the HNG-X system. Therefore, providing a domain overlay to the network tier model is provided to assist with understanding the demarcation points and perimeter defences. Figure 3 (taken from the HNG-X Technical Network Architecture document) highlights the access and enforcement points.

POL00398165

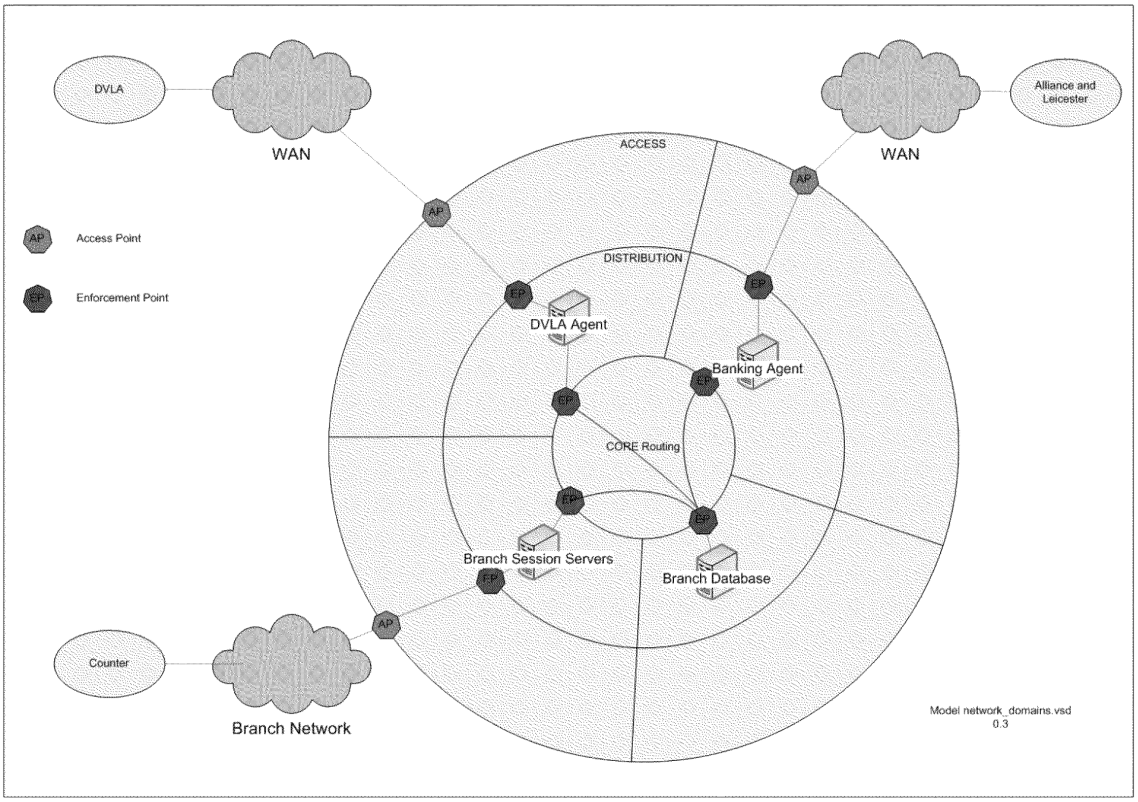

Figure 3 – Network Tier Model Overlay

4.2.1 Access and Enforcement Points

The security of the network is built around determining where the various access and enforcement points are located and if the network components within these areas are suitable and configured correctly to maintain the integrity of the system.

4.2.1.1 Access Point

This is the point of entry from the WAN for all traffic. It resides within the Access tier of the network and would expect to be a network device that interfaces between the LAN and WAN.

4.2.1.2 Enforcement Point

This lies on the boundary between the access and distribution tier, and as shown within the architecture design comprises of a firewall. The Cisco Adaptive Security Appliance (ASA) 5540 series appliance is the device that provides the protection and control. All traffic will pass through this component and any traffic that flows between domains will need to pass through. The firewall will only have one interface within any one network tier. In the case of the ASA one interface will belong to the access tier and the other will belong to the distribution tier.

POL00398165

4.2.2 Network Threats

4.2.2.1 Potential Malicious Progams and Tools

The HNG-X network must be secured against the threats and infiltration methods. There are many potentials ways of either maliciously attacking the HNG-X network in order to make it inoperable. Below are but a small number of network infiltration methods which could be used to infect the HNG-X systems:

- **Virus**
- **Worm**
- **Trojan**
- **Spyware/Adware**
- **Phishing**
- **Spam**
- **Bot**

4.2.2.2 Types of Network and System Attacks

The HNG-X system must enforce security policies so that is protected from potential internal or external attacks. These threats can take various forms. The system attacks i.e server and end user may be affected due to a perpetrator using some of the malicious programs available, as identified at 4.2.2.1. The following list identifies some of the types of attacks that the HNG-X network needs to protect itself from, which ultimately affects the network and therefore renders the system unusable. Some of which are well known due to previous Internet exploitation:

- **Distributed Denial of Service (DDoS)** where massive amounts of traffic sent to number of targets within short space of time
- **Denial of Service(DoS)** where there is an attempt to stop legitimate users of a service from accessing that service using software bugs i.e. IP Spoofing
- **Man in the Middle Attack (MITM)** where an attacker can read, insert, modify messages between two parties with neither party aware that the link has been compromised.

4.2.2.2.1 Denial of Service attack – IP Spoofing

This can occur when an intruder sends a message or large amount of UDP echo traffic to IP broadcast address which then causes all replies to be a particular spoofed source address i.e “Fraggle” attack

4.2.2.2.2 Man in the Middle attack – ARP spoofing

This is when a host sends an ARP request to the gateway router and an attacker sends an ARP response to a host with the attacker’s MAC address instead of the expected gateway router’s MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

POL00398165

4.3 DMZ's

The DMZ's in HNG-X provide another layer of protection for the Core system. Isolating initial authentication, logon and DC service from with the Core infrastructure clearly limits the potential for security violations. Trusted and less trusted interfaces provide the necessary security and traffic flows are limited to the configurations permitted via the Cisco ASA appliance. Standard security rules apply, namely that traffic /sessions are only initiated from within a trusted zone; inside to outside. The inherent design of the firewall is to prevent any outside traffic/device access to an inside domain/LAN and therefore traffic from the outside that needs to communicate with the relevant DMZ will need to be explicitly permitted with the firewall's (ASA's) configuration.

4.3.1 Security Levels

The DMZ's Cisco ASA's has default parameters that set the security levels so setting up of connections and passing of traffic for particular paths need to be configured specifically. In the case of the HNG-X DMZ's the ASA will be configured with an outside, inside and DMZ interface. These interfaces will need their security levels set to reflect their trustworthiness and to enable the firewall configurations to work correctly. See Table 1

Interface	Security Level
Inside interface	100 (default)
Outside Interface	0 (default)
DMZ interface	0 by default , set to 50 (configurable)

Table 1 - Security Levels on ASA

Access tier has a number of DMZ's with trusted, less trusted interfaces. Default policy is that any ASA appliance/firewall protecting the DMZ will allow connection allowed from inside to outside, but implicit deny all on the outside.

To overcome this restriction and to allow incoming connections specific ACL rule sets, static routes and NAT statements will need to be configured on the ASA. Exact configuration setting will need to be identified in the Firewall LLD and the firewall workshop.

4.3.2 Types of DMZ for HNG-X Architecture

The DMZs for HNG-X are split into multiple areas. Services that are provided here are authentication, remote logon and SSL termination and are provided by RADIUS, RSA and SAS servers.

- Post Office DMZ
- Branch DMZ
- Clients DMZ
- Support DMZ

POL00398165

4.4 Data Centre LANs and Server Services

The DMZ's protect the servers and services that support HNG-X. It is these servers that will determine firewall rule sets as they provide the source and destination addresses and protocols for traffic flows. The following Table 2, taken from DES/NET/HLD/0008 shows server/platform types and associated DMZ.

Zone	Domain	Systems / Platform types
A	Estate & Systems Management LAN	Tivoli Servers Anti-Virus Server
B	Central LAN	Other servers with no specific security segregation requirement. ie DNS servers, Active Directory servers.
C	Certificate & Key Management LAN	Certificate Server, Signing Server Key Management System
D	Audit LAN	Audit Server, Audit Workstation, Atalla Device
E	Database Servers LAN	Branch Database, TES, NPS,DRS,TPS, DWh
F	Management Services LAN	NNM / OVO server CiscoWorks server, TACACs+ server AlarmPoint server, NTP server Cisco Security Manager server Aurora console server RSA EnVision logging server
G	Post Office DMZ	POL MIS, POL FS TES Application Server
H	Branch DMZ	Branch Access, SSL VPN Termination Branch Access Layer Application Servers Branch Router RADIUS Authentication Server SYSMAN Gateways
I	Clients DMZ	Client Agents Network Banking Atalla Devices FTMS Agents
J	Support DMZ	RSA Authentication Servers SAS Servers Out of Hours remote access

Table 2 - Data Centre domain platform components

POL00398165

4.5 Services Requirements

The services provided by the HNG-X systems are:

- Identity and Audit
- Network Management
- IPSEC
- SSL

4.5.1 Identity and Audit

All logon activities within the HNG-X domain, internal to datacentre or at remote sites i.e Branch or Clients (DVLA, Alliance and Leicester etc) will need authentication and role authorisation, and accounting. This is based on the AAA model. This includes either endpoint logon or network device logon.

The servers providing user and network logon security are as follows:

- Cisco ACS located in Management Services LAN
- SAS server located in Support DMZ
- Radiator RADIUS Branch Authentication server

4.5.1.1 Integration with Active Directory

The logon process is securely tied in with Active Directory whereby username and passwords are backed off from the ACS server. This extra hop in terms of authentication and authorisation provides an extra level of security. For information on the process can be found within X (doc to be determined)

4.5.1.2 Cisco ACS

Cisco ACS (Access Control Server) is the device that provides the focal point for user and device management across the HNG-X system.

- ACS establishes a common user and device AAA management framework for protecting and monitoring user and device access in the network for example:
    - ACS controls who can log into the network
    - The privileges of each user, and what they can and can't do
    - Recorded security audit or account billing information
    - Access and command controls that are enabled for each configuration's administrator
    - ACS allows management and user access for all the Cisco devices within the HNG-X system

POL00398165

4.5.1.3 Summary of Logon

Device	Action	Protocol Used	Security mechanism	Location	Notes
Network Components - Cisco	Logon to network device is via the LAN interface.	SSH	Via SAS Server through IPSEC VPN	Support DMZ	
Network Components – Cisco	Authentication of User Logon	TACACs+	ACS Server + Usernames in Active Directory (AD)	Management LAN	Two Factor authentication
Branch Router - Sarian	Logon to network device is via the WAN interface	http/telnet	IPSEC via Sarian Head End router in datacentre	Branch DMZ	Single factor authentication
Branch Router - Sarian	Authentication of User Logon or loading of config from bootserver	RADIUS	RADIUS Radiator server + Usernames in Active Directory (AD)	Branch DMZ	

Table 3 – Logon Summary Matrix

4.5.1.4 System unavailable for logon

In the event of system being unavailable to authenticate there are two options:

- Network device local logon
- Local console logon

4.5.1.4.1 Network Device local logon

In the event of system being unavailable to authenticate, the security policy permits that a device can be configured for a local account so that authentication can take place locally and user access levels are assigned based on the role of the user. These access levels within Cisco devices are known as user exec mode and privilege exec mode.

4.5.1.4.2 Local Console logon

As a last resort for engineer access a device can be administered via the console port. The security principles that need be in place and allow this are :

- Generic username with a separate last resort password per device

POL00398165

- When password used then it is changed
- Key under lock and key

4.5.2 Command Audit

All commands issued by the users when they are logged in to network components are logged. The logging is performed by:

- ACS logging
- Aurora logging

4.5.3 Network Management

Network management for Cisco devices and Counters is undertaken securely from Management LAN and Support DMZ via SNMPv3, SSH version 2, or HTTP over SSL. Activities include:

- Device monitoring
- Uploading of Configurations

4.5.3.1 Branch Router

The Branch Sarian router is managed by the ROSS platform (Router operational support system). The Sarian router supports telnet, ftp and http, which is clearly insecure. To overcome this security issue these protocols are run over IPSec tunnels that are established from the VPN client on the ROSS platform to the Sarian IPSec head router in the DataCentre, and then onwards to the Branch router.

ROSS platform also provides NTP service for Branch router via SNTP service via IPSEC tunnel.

4.5.3.2 Other Security Criteria to be met

- No clear text passwords will be used
- Firewall management will use https and ASDM + Cisco Security Manager
- All network devices will be deployed with parameters set for logging and alerting. This requirement is achieved by carrying out baseline configuration tasks.

4.5.3.3 Logging

The security policy is that all devices will be configured for logging, and these logs are maintained by CiscoWorks, Network Node Manager and RSA Envision logging server.

4.5.3.4 Alerting

The security policy is that all devices will be configured for alerting using SNMP v3. Alerts will also be directed towards CiscoWorks and Network Node Manager in the Management Services LAN which will then feed into the Enterprise Management System which is supported by a 24 hour helpdesk.

POL00398165

4.5.4 IPSEC

IPSec has multiple configuration requirements due its stepped approach. The security policy is to use the strongest encryption and authentication configuration that is possible, on the basis that the deployed network devices support the current technologies and security enhancements.

IPSec will be configured between

- Sarian VPN concentrators and Sarian Routers for Management of Branch routers
- On Handoff 2811s at Datacentre and at the remote sites for Client, Post Office, DVLA, A+L for production traffic and management traffic (for network devices)

HNG-X IPSec policy is to encrypt all traffic; by default this means that all traffic is deemed interesting.

The parameters below will be used for both LIVE and TEST traffic.

4.5.4.1 Parameters

The security parameters that are to be used by default as part of the IPSec configuration on the network devices are as follows:

General Parameter	Weak	Stronger	HNG-X configuration parameters
Encryption Algorithm	DES	3DES or AES	AES with 256-bit key
Hash Algorithm	MD5	SHA-1	SHA-1
Authentication method	Pre-share	RSA Signature	Pre-share or RSA Signature (TBD)
Key Exchange	DH Group 1	DH Group 5	DH Group 5
IKE SA lifetime	86,400 secs	<86,400 secs	Set to < 1day, limit to 4 hours (TBD)

4.5.5 SSL

This is more specific to the Branch counters whose security is provided by the Sarian Router and IPSEC headend at the HNG-X datacentre and the client application on the counters.

All transaction data travels over SSL which has the secured communications via the IPSEC tunnels.

This SSL transport is then terminated on the Cisco 6513 Access switch in the Datacentre via a Cisco ACE blade module which supports SSL terminations.

HTTPS (TCP 443) is required to be permitted through controlling network devices.

The Network administrator will generate the private/public key pair for the router. The private key cannot be seen by anyone, including the administrator. The Certificate server will be a central authority for deciding whom to issue, revoke, etc. the certificates. This server will be managed by the Crypto team providing a clear separation of management.

4.6 Key Management/Certificates/PSK

This element of the solution that provides authentication is via Certificate servers located in the Central LAN. As explained previously all communications will take place over a secure path,

POL00398165

IPSEC tunnel. Therefore, certificate integrity and management is regarded as safe. The assumption is that the certificate server has not been compromised itself.

4.7 Traffic Types

The network devices deployed can each be divided up into the following functional components:

- Data Plane
- Control and Management Plane

4.7.1 Data Plane Traffic

This is concerned with the type of application traffic and the direction it is looking to flow. Within the Datacentre there are numerous servers that are located in the Access and Distribution tiers that will need to communicate with each other as part of their system function. As both tiers are separated by either an FWSM or ASA, rule sets will have an impact on data traffic flow. Ultimately a security device will be configured to allow certain traffic pass through; this information should be available from the server and application HLD's or obtained by holding a suitable workshop on server traffic flows. An example of information that may need to be considered from the workshop is shown in Table 4 below

.

Source Domain	**Systems / Platform types**	**Destination Domain/LAN/Devices**	***Service being provided***	***Protocols required***
Certificate & Key Management LAN	Certificate Server Key Management System Signing Server	*i.e.Counter*	*Digital Certificate/2 factor Authentication*	*X509*
Estate & Systems Management LAN	Tivoli Servers, Anti-Virus Server	*i.e all LANs*	*Software, Anti virus service*	*TBA*
Central LAN	DNS servers, Active Directory servers.	*i.e DMZ servers*	*DNS*	*DNS, netbios,LDAP?*
Management Services LAN	CiscoWorks server TACACS+ server RSA EnVision logging server	*i.e Counters, all Network Devices*	*TACAC+ for device authentication, user authorisation*	*TACACs+ (TCP 49)* *SNMP, SSH, NTP, SYSLOG, PING*

Table 4 – SAMPLE Inter LAN/Domain Protocol Matrix

POL00398165

4.7.1.1 Data Traffic Separation

As stated above this will need to be derived from an appropriate workshop or via other HLDs

4.7.1.1.1 Access Tier – LAN side

Will be controlled with the use of VLANs whereby traffic classes i.e DVLA, CAPO, LINK and Support are separated into different VLANs and ports on the Access 6513 configured accordingly.

4.7.1.1.2 Access Tier – WAN side

Will be controlled via dedicated MPLS VPN, dedicated IPSEC tunnel over shared MPLS VLAN or dedicated circuits

4.7.2 Control and Management Plane Traffic

Most traffic passing through a network device does so via the data plane. However, the HNG-X active devices will needs to handle certain packets, such as routing updates, keepalives, and network management which are known as control and management traffic.

The route processor on any of the HNG-X network devices need to be protected from possible network attacks such as DoS, whereby high rates of route processor destined traffic cause an excessive amount of CPU utilisation on the route processor.

It is critical that the functionality and integrity of the network device is maintained as any impact on the network device from a DoS attack will clearly have an impact on the business. To alleviate this concern it is advisable that a policy to police the type of traffic entering a network device is created.

4.7.2.1 Control Plane Policing Policy

The HNG-X system integrity and functionality is reliant on active components behaving as expected. Preventing DoS and other attacks is crucial to the business. Identifying a number of traffic classes will assist in securing the system as these classes of traffic can be monitored and traffic not expected will be denied. Even though an appropriate workshop may be, the following requirements should be considered:

- Critical traffic such as routing protocols i.e. OSPF and RIP
- Important traffic such a network management traffic i.e ssh, telnet, ntp, snmp
- Normal traffic such as ping (icmp echo request)
- Undesirable traffic i.e. any known malicious traffic
- Default traffic i.e. any other traffic not previously captured

4.7.2.2 HNG-X Traffic Policing

This element of network security will be undertaken by the 6513's in both the Core and Access Tiers.

- Limitations will be placed on the types and rates of packets that can consume CPU resource. i.e for example fragmented ICMP echo requests

POL00398165

- Traffic storm control will be configured on the switches with the threshold to be determined.

4.8 Traffic Classes and Traffic flows

4.8.1 Traffic Flows and Classes

Traffic Flows fall into the following 3 categories:

- Management
- Production
- Test

Traffic Classes fall into multiple categories based on the clients. The comprehensive list is found within the HNG-X Technical Network Architecture, but two examples are:

- EPAY LIVE and EPAY Test
- DVLA LIVE and DVLA Test

4.8.1.1 Security Policy for Traffic Flows

Identification of traffic flows and general server to server communication will provide the necessary port and protocol information for the creation of LLDs. This information, such as permitting only certain TCP ports to be opened between two servers needs to be determined and should be provided by server and application HLDs. It may be that some form of workshop will be held to identify these requirements.

Expected level of information based on port, protocol, and IP addresses will then allow the creation of the rule sets for devices.

The fundamental security policy and configuration should be the same for all classes, namely

1. Allow only very specific traffic based on source, destination IP address and protocol
2. Deny any other traffic.

4.8.2 Network Appliance Rule sets

Proactive network security is ultimately provided by the network components deployed which, in the case of the HNG-X solution covers ASA, IPS, Routers with ACLs and Cisco ACS. Rule sets configured on these devices are the security mechanism used to isolate and drop unwanted and unknown traffic, report on potential security violations and offer a robust defence to network threats.

Determining the precise rule set for the components should become known as the system is built, and should be seen as a list that will be updated regularly as new vulnerabilities and change to requirements are understood. The LLD for the particular components will indicate the protocols and parameters for the rule sets which should be collated as part of a security workshop. The format that the rule sets will take will be as per the following criteria:

- Allowed traffic i.e expected traffic such as https port no 443

POL00398165

- Denied traffic i.e. source IP address denied
- Logged traffic i.e. denied traffic logged to syslog server
- Accepted signatures (IPS/IDS)

4.8.3 Device Matrix for Traffic Flows

Below Table 5 provides a summary guide for the specific LLDs to protect the HNG-X network. It should be used in conjunction with any workshop on traffic flows and firewall filtering.

Protection Device	Location	Protection Mechanism	Traffic Flow /Type	Source LAN	Destination LAN	Config Specifics	Rules
Cisco ASA	Access Tier – Zone 1	Application Procotol filtering	Inbound to DMZs	Counter	Branch DMZ??	NAT rules Inspection types Static routes	Permit counter addresses Deny all other addresses Permit SSL
Cisco ASA	Access Tier – Zone 1	Application Procotol filtering	Inbound to DMZs	Remote Sites	Client DMZ		Permit LAN addresses Deny all other addresses
Cisco ASA	Access Tier – Zone 1	Application Procotol filtering	Inbound to DMZs	Support locations	Support DMZ		Permit Support LAN IP addresses Deny all other addresses
Sarian Router/VPN concentrator	Access Tier	Packet Filtering ACL	Outbound from Sarain HeadEnd	Access LAN	Branch router	ACLs	Allow telnet , ftp
Cisco ACE blade	Access Tier	TBA	SSL	Counter	Access LAN	TBA	Permit SSL
McAfee IPS 3000 sensor	CoreTier	Siganature, Anomalies to traffic flow	Inbound to Core from Access Tier	Access LAN	Core LANs	Signature matching / updates	Match signatures, observe and permit/deny anomalous traffic
Cisco Firewall Services Module (FWSM)	Core Tier – Zone 2	ACLs	Inbound to Core from Access Tier	Access LAN	Core LANs	ACLs	Permit/deny accls based on source/destination and protocol port number

Table 5 – Device Matrix for Traffic Flows

POL00398165

4.9 Security Components

Across HNG-X a variety of security barriers and data protection methods are to be deployed to protect the infrastructure and systems. These are as follows:

- ASA Firewalls
- Cisco Routers with ACLs
- Sarian VPN Concentrators and Routers
- IPS/IDS appliance
- SSL
- VPN tunnels with valid encryption and authentication

4.9.1 HNG-X Network Security Devices

Table 6 lists the device to be deployed, their location/domain and the security criteria they will meet

Network Security Device	Access or Enforcement Point	Location	Domain	Network Tier	Security criteria
Sarian Router/VPN concentrator	Access Point	Data Centre	Branch	Access	IPSEC tunnels
Cisco ACE blade	Access Point	6513 Access switch	Branch	Access	SSL termination
Cisco Adaptive Security Appliance (ASA)	Enforcement Point	Data Centre	Branch	Access/Distribution	Application + protocol filtering, IPSec VPN, IP address ranges, protocols and ports.
McAfee IPS 2700 sensor	Enforcement Point	Data Centre	Branch	Distribution	Signature, Anomaly, DoS Detection and Prevention,
Firewall Services Module (FWSM)	Enforcement Point	Data Centre	Branch	Core	Firewall based rules
SAS server	Access	Datacentre	Support DMZ	Access	Application level firewall

Table 6 – Network Security Devices

POL00398165

4.9.1.1 Device Details

4.9.1.1.1 Cisco 2811

Known as Handoff routers and used to supply IPSEC tunnel connectivity between the Datacentre and FJ RMGA LANS, (red LAN), Corporate LAN, DVLA, EPAY, Post Office sites, Support, Internet Access via SDC01. The IPSEC tunnel also passes through a C+W VPN tunnel.

The 2811 also provide Datacentre LAN connectivity into the Access switch 6513's.

4.9.1.1.2 McAfee IPS/IDS 3000 Sensor

The McAfee IPS/IDS 3000 Sensor has been chosen as the skill set for supporting this device is available within Fujitsu.

It will act as a security barrier by using both its IPS and IDS capabilities.

- IPS Mode – Used only for Branch traffic monitoring
- IDS Mode – Used to monitor all other traffic flowing in Core and Access tier.

IPS Mode places the sensor inline and therefore is seen as an active device in the traffic path for Branch traffic all traffic flowing between the Branch counters and the Core and Access tiers. The traffic is inspected as it arrives on one interface and exits on the other. Any malicious traffic will be denied and an alert sent to the syslog server and its own Management station located in Management Service LAN .Subsequent malicious traffic will be blocked due to the IPS's proactive capability.

IDS mode will be utilised for remaining flows, and will monitor the traffic by using SPAN ports connected to Core and Access. Any alert notifications will be sent to its Management station.

Active/Standby configuration will be deployed whereby all traffic is examined by the primary sensor with the secondary remaining inactive until a failover scenario is invoked.

Sensor Management will be via McAfee Intrushield software that will be installed on a dedicated server in the Management LAN. Access to the sensors for general management, signature and software updates will be via this management server.

Signature updates are expected to take place weekly whilst only a maximum of two software upgrades are ever likely to be required within any one year (if required at all).

Expected positioning of the sensor is shown in Figure 4

POL00398165

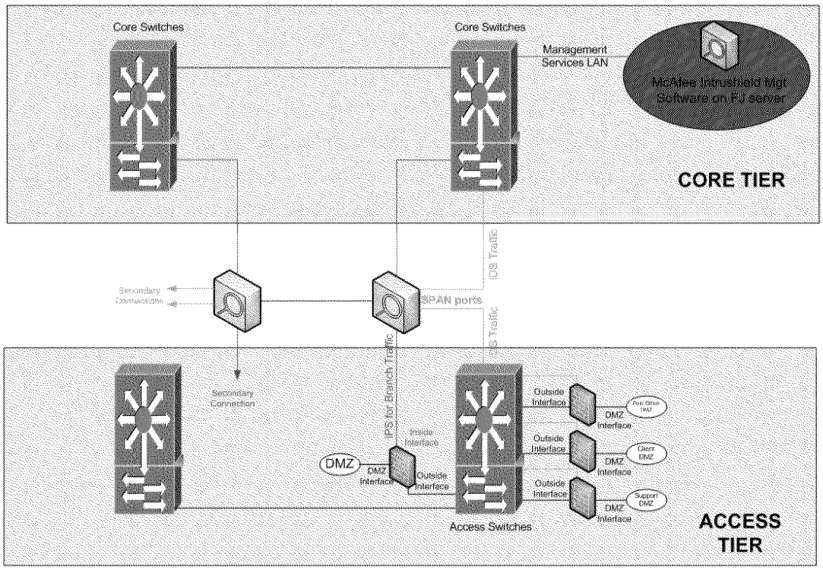

Figure 4 – McAfee IPS/IDS Positioning

DN: FURTHER INFO from IPS source expected to be added

4.9.1.1.3 Cisco Adaptive Security Appliance

This is used to ensure that traffic traversing out of the Cisco 6513 Access switches is valid. They provide the route to the Demilitarised Zones (DMZs) for all the domains such as Post Office, Branch, Clients, Support and within each of these DMZ's there are platforms such as Branch application servers and Branch Router RADIUS authentication servers.

The default configuration of this appliance will be to ensure that no traffic is permitted to pass through unless explicitly permitted. This security stance adheres to the principle stated within Section 1.8 that states that traffic "which is not explicitly granted is denied". Workshops to identify actual traffic flow will provide the protocol and port information necessary to configure the devices.

4.9.1.1.4 Cisco ACE

This blade provides server load balancing and virtualisation. It takes over the functions of a separate SSL devices and has security functions that otherwise would have been provided by multiple devices.

It provides the termination point for counter SSL sessions from the counter HTTP client into the Branch session servers.

DN: FURTHER INFO may be required on the ACE if not covered with Datacentre HLD

POL00398165

4.9.1.1.5 Cisco Firewall Services Module

Housed within the Core 6513 switches it provides another layer of security and protection to the Core servers. As another layer of protection that promotes the security policy of providing 'defence in depth' it has been chosen as it is fully supportable as part of the managed service and protects the Core from any security violation from within the Access tier.

This integrated module can be configured with up to 100 separate security contexts. A security context is a virtual firewall that has its own security policy and interfaces. Having multiple contexts is similar to having multiple stand-alone firewalls.

Configuration Rules for the FWSM

1. The policy of protection based on source IP address and Destination IP address and TCP/UDP ports will be followed.

4.10 Network Attack Prevention Techniques

The main aim of the HNG-X network security is to prevent attacks that impact the business or the support of the business. There must be mechanisms in place to counter act the threat. For the likes of DoS and MITM attacks hardware and software configuration including authentication techniques are core to providing system and network integrity, functionality and retaining business continuity. The following are examples of mitigation techniques that should be considered within the HNG-X network to prevent either a DoS or MITM attack:

- Disabling 'IP directed broadcast' for DoS attack
- Enabling 'ARP inspection' for MITM attack
- Enabling 'Reverse Path Forwarding' for IP Spoof attack

4.10.1 Disabling IP directed broadcast

Disabling 'IP directed broadcast' denies IP broadcast traffic onto a network from other networks. This action should be considered as the default for any routers within the HNG-X network. System and server interaction may require some IP broadcast functionality; if this is found to be the case then appropriate ACL's should be applied to each interface on which specific directed broadcasts are to be enabled. This feature is disabled as part of Cisco "AutoSecure" as identified in Appendix B.

4.10.2 Enabling ARP Inspection

ARP inspection ensures that an attacker cannot send an ARP response with the attacker's MAC address so long as the correct MAC and associated IP address are in the ASA's static ARP table.

By enabling ARP inspection on ASA firewall, the MAC address, IP address and source interface in all ARP packets are compared to static entries in the ARP table, and an action of permit or deny carried out.

4.10.3 Enabling Reverse Path Forwarding

By using the "ip verify reverse-path interface if_name" on the firewalls a spoofed source address can be detected. The firewall examines the source address of each packet and checks in its

POL00398165

routing table that there is a route present (as if to send the packet back). If the route isn't present or the reverse path interface doesn't match the arriving interface, the packet is dropped and a logging message generated.

4.11 HNG-X Firewalls

These are two types of firewall deployed in the HNG-X network:

- Internal – as a FWSM blade in the Core 6513s within the Core Tier
- External - as an ASA 5540 appliance for each DMZ that exists within the Access tier, namely,
    - Post Office, Client, Branch and Support.

The ASA 5540's are capable of delivering some of the following features:

- high performance and high density security services
- provide up to 650Mbps firewall throughput
- 400,000 concurrent connections

4.11.1 Advanced Protocol Handling

The HNG-X ASA devices can provide layer 3, 4 and 7protection. The minimum requirement is that all firewalls are configured to permit or deny on IP address and/or TCP or UDP port number. Extra protection can be provided by configuring the ASA to inspect packets at Application level and to permit or deny based on the set criteria.

The ASA firewalls should be configured to inspect packets above the network layer. This will cater for those applications such as FTP, HTTP, multimedia and SQL that require their communication protocols to dynamically negotiate source or destination ports or IP addresses.

The ASA supports Application Inspection by using the advanced protocol inspection algorithm which ensures the secure use of applications and services. If a secondary TCP or UDP port is used to transport data between a client and server then the application inspection function monitors the sessions and permits data exchange on the dynamically assigned ports whilst the session is open.

4.11.1.1 Security Benefit of Protocol Handling

From a network security perspective it:

- Securely opens and closes negotiated ports and IP addresses for legitimate client-server connections through the ASA
- Inspects packets for signs of malicious application misuse

4.11.1.2 Configuration Policy for Application Inspection on HNG-X

The ASA firewall has a preconfigured global policy that enables inspection of certain applications on all interfaces based on well known applications and their ports. This default inspection traffic class will be used at the implementation stage, and therefore requires no immediate firewall configuration.

POL00398165

In the event that a less well known application is identified later in the implementation cycle the inspection policy can be amended accordingly by the network security team managing the device.

4.11.2 Firewall Zones

The ASA and FWSM firewalls are positioned within the HNG-X datacentre and perform protection for different traffic flows. For ease of specifying rule sets they can be seen as being located in two zones, 1 and 2. This is identified below:

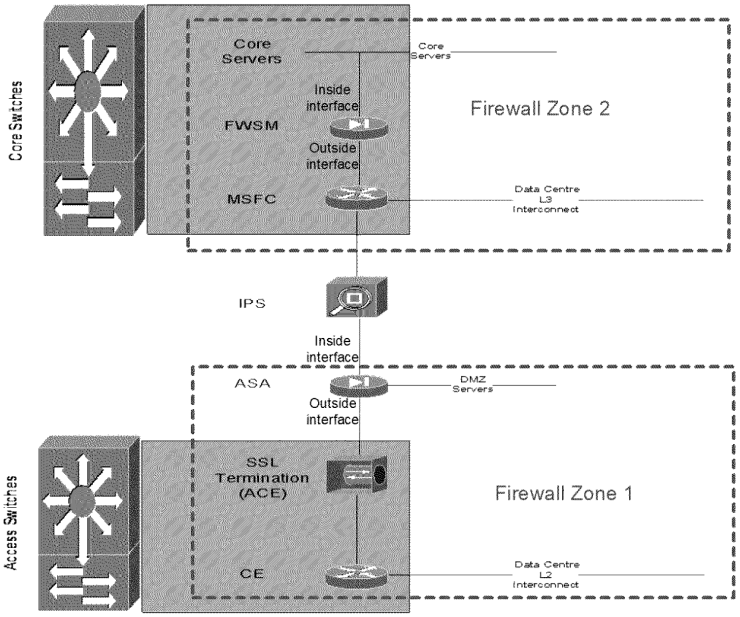

Figure 5 – Firewall Zone

4.12 Firewall Based Rule Set

This HLD does not provide comprehensive rules sets for all traffic flows as it is not deemed to be an appropriate document for recording of such information. However, a guideline on their creation is needed and ongoing operational use is required so the following should be considered

Two elements are considered for this.

- That there is a base configuration or approach to be applied to all firewalls, be it a blade or appliance.
- Each firewall will have more specific rules dependent on their positioning and the traffic they are expected to deny or allow.
- It is expected that the firewall rule sets and traffic flows are identified in a working document or spreadsheet that will be used by operational staff and is under appropriate change control. As a guideline Appendix C provides both an overview of expected traffic flows. This could be used as a basis for identifying traffic flows at an appropriate workshop and/or at system build stage.

POL00398165

- As a high number of protocols across the whole of HNG-X system are required for system functionality and that these are currently not identified within Application HLDs it is recommended that a workshop and a protocol capture activity is undertaken during system build stage.

4.12.1 Firewall Configuration

The ASA 5540 devices are positioned in pairs as a Hardware Failover Active/Standby configuration with Stateful failover and can be configured with separate contexts, if required.

All firewall configuration (and management) must be undertaken via Cisco Security Manager.

4.12.1.1 General global parameters

The LLD's for firewalls should ensure that the following security guidelines are adhered to:

- SSHv2 is permitted inbound for Management purposes with following parameters
  - Public key generation
  - Domain name
  - IP address of ssh client
  - Idle time out set to default of 5 mins
  - AAA authentication
- NTP is permitted in and outbound of the firewall to the recognised time source server in the Management Services LAN to allow for time synchronisation
- Syslog traffic is permitted outbound from each firewall to the syslog server
- SNMP v3 (TCP/UDP 161) is permitted outbound from each firewall to the Alert Management Server
- Traffic required for systems involved in Window Shares to be permitted
- Object groups will be created to group devices (servers and network components) based on network address group i.e. subnets, protocols and services.
- It is acceptable to use a subnet mask that covers a range of addresses even if there is no IP address within that range allocated to a device. This will simplify the base rule set by not having individual rules created and ultimately avoids large configuration files.
- All traffic that attempts to pass through the firewall, yet fails due to the access rules is still logged. The aim is to "capture all denies and log"
- A timeout threshold on connections between source and destination is set. With the stateful configuration of the firewall a valid connection could be opened and maintained indefinitely subject to traffic being sent. The threshold for any connection will remain at default, but are configurable if necessary. See Table 7

Thresholds description	Default Time Out Settings	HNG-X Timeout settings	Configurable Settings
TCP connection	1 hour	1 hour	To minimum of 5 mins
XLATE table	3 hours	3 hours	To minimum of 1 min

POL00398165

Thresholds description	Default Time Out Settings	HNG-X Timeout settings	Configurable Settings
Embryonic half closed connections	10 minutes	10 minutes	To minimum of 5 mins
UDP connection	2 minutes	2 minutes	To minimum of 1 min

Table 7 - Firewall Thresholds

4.12.1.2 Interface configuration

The ASA 5540 appliance supports the use of sub-interfaces and as a high performing device can be used to deliver a number of the HNG-X services. In terms of interface connectivity and configuration the following policies should be used (Summarised in Table 8)

- An ASA will be used for multiple connections/clients. i.e it will not solely be used for DVLA, but will protect inbound DVLA, EPAY etc traffic. See **Error! Reference source not found.**
- As each ASA has been purchased with 4*GE and 1*FE interfaces then the gigabit interfaces should be used first. Table 8 below indicates recommended settings per ASA.
- All interfaces must have their speeds specified, and therefore the auto option is not used.
- Stateful failover requires an Ethernet interface with minimum speed of 100Mbps (always use Gigabit if available)
- The ASA should be configured to allow for encrypted and authenticated communication between failover pairs using the “failover key” command
- The outside interface that connects to connects to the access 6513 switch will be configured to support sub-interfaces
- The inside interface that connects to the Core 6513 switch will be configured to support sub-interfaces
- The DMZ interface that connects to the DMZ(s) will be configured to support sub-interfaces.
- Security Level Conventions will be used
- Any unused interfaces should not be configured and left in a “shutdown” state

Interface	Position	Use of Interface	Interface Speed	Duplex Settings (auto/manual)	Interface Capability	Security Level	Interface Attributes	Other Information
0	Outside	User Traffic	Gigabit	Manual	Sub-Interfaced	0	Named(linked to IP add)*	
1	Inside	User Traffic	Gigabit	Manual	Sub-Interfaced	100	Named(linked to IP add)*	
2	DMZ	User Traffic	Gigabit	Manual	Sub-Interfaced	Between 1-99	Named(linked to IP add)*	
3	Mgt	Mgt and Stateful	Gigabit	Manual	Normal	N/A	Named(linked to	Use encryption

POL00398165

Interface	Position	Use of Interface	Interface Speed	Duplex Settings (auto/manual)	Interface Capability	Security Level	Interface Attributes	Other Information
		Failover					IP add)*	and authentication for failover using "failover key"

* This assists with the configuration process, especially when using object groups. Names should be logical and meaningful

Table 8 – Interface Settings

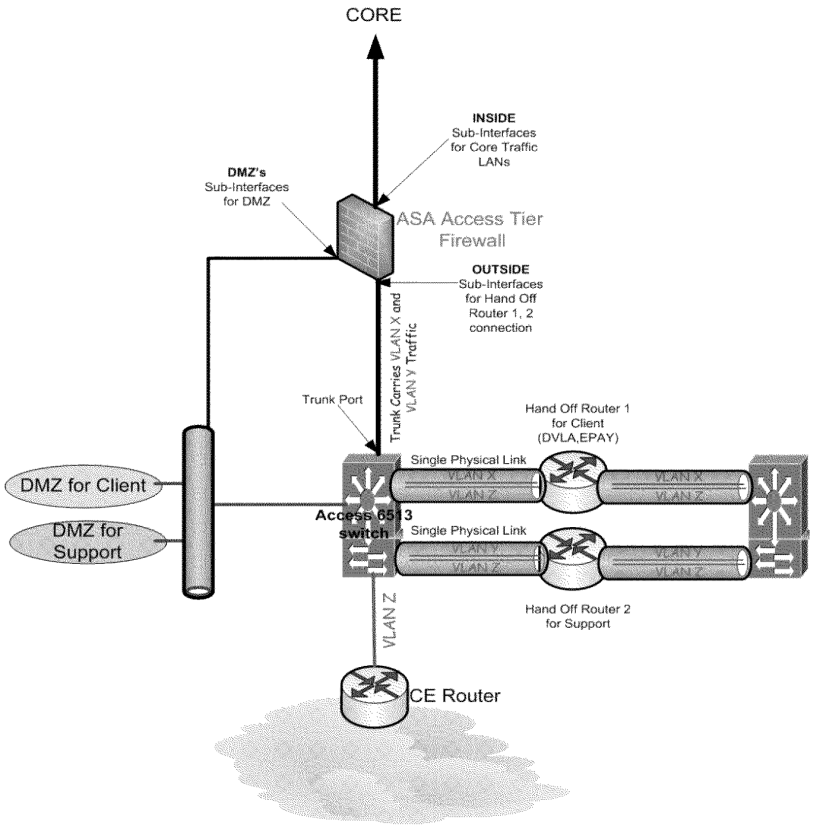

Figure 6 – ASA DMZ Connectivity

4.12.2 Sample Specific Rules for Firewalls

Precise firewall rule sets will require detailed investigation of the traffic flows and understanding of the application traffic and protocols in use. This information needs to be obtained from the

POL00398165

relevant application and server HLD's in order that protocol matrix can be created. This is an ongoing activity. Table 9 shows an example of the type of information expected in the matrix:

Firewall	Zone	Location	Source/IP	Destination/IP	Protocol	Permit/Deny	Interface
ASA 1 Pair	1	Access Tier	Counter	Branch DMZ - Authentication Server	RADIUS UDP 1812,1813	Permit	Outside inside
FWSM	2	Core Tier	Ciscoworks	Remote Client LAN	SNMP	permit	Outside inside

Table 9 - Firewall Matrix

4.12.2.1 Configuration for Corporate Firewalls

These will need to be amended to include any new HNG-X address ranges and to permit routing paths.

4.12.2.2 Configuration for Remote Firewalls

Remote firewalls such as the Branch Sarian router will need to be configured to allow HNG-X Datacentre traffic through.

4.13 Network Controls

Network controls will use the methods below:

- Physical access , lock and key
- Network Separation– Physical and Logical
- VLANs – VACLs, Private VLANs, Limiting trunk ports
- Router ACLs
- Network Device Lockdown - Cisco "Autosecure"
- NSA regulations
- Device Operating System i.e Cryptographic Image

4.13.1 Physical Access, Lock and Key

This should be mandated as part of the overall security policy. Ensuring physical access is limited to authorised personnel will minimise the risk of a network breach, and should be considered the first line of defence.

Physical access into an area, be it Datacentre or at a remote location will be controlled. Specific access controls per site are unknown as they are out of scope of this document but they expected to be based on the following:

- Swipe Card Access
- Standard Key Access

POL00398165

- Access logs maintained
- Required Security Levels of Personnel met
- Location access/ computer room access limited to authorised personnel
- Network devices installed in designated network racks which are locked and the key maintained by appropriate personnel
- Procedures for logging access should be enforced based on local and Project security policy.

4.13.2 Network Separation

4.13.2.1 Physical Separation

The nature of the HNG-X architecture means that network segmentation is in place by default. It is physically segmented due to the components that will be in use i.e ASA firewall, routers, and switches.

4.13.2.2 Logical Separation

This is provided by using VLANs.

4.13.3 VLANS – VACLs, PVLANs

This method of network separation provides the following benefits:

- Limits broadcast domain and therefore ARP attacks
- Logically separates out traffic into different subnets whilst retaining same physical location for devices
- VLANs can have access controls easily applied which offers another prevention mechanism.

Even within the same server farm i.e the same broadcast domain there may be a requirement to isolate one server from another to minimise the risk of an attack from a valid source that has been compromised. Mitigating controls that should be implemented are Private VLANs, VACLs and manual configuration of VLANs on trunk ports.

4.13.3.1 Private VLANs

Servers can be protected from attack from other servers within their own VLAN with use of Private VLANs. This security capability is useful especially if one of the servers within the subnet has already been compromised, and is to be used to launch a network attack.

All the DMZ's for the Branch, Client and Support remote networks have a number of servers that offer services. These servers may or may not need to communicate with each other. If they do not then it is good practice to configure the access switch/network connection for Private VLANs.

The security recommendation is to isolate the DMZ servers at Layer 2 (subject to any workshop identifying the need for servers to communicate with each other).

4.13.3.2 VACLs

POL00398165

These VLAN Access control lists filter the traffic that may go between VLANs and add an extra security barrier between end stations. Determining what, if any VLANs are access list controlled is dependent on the traffic flows between servers. Again, this level of detail that needs to be identified for any switch LLD, should be made available once a valid server/DMZ workshop has been undertaken.

4.13.3.3 Trunk Port VLAN Configuration

Base switch configurations should ensure that all trunked ports are limited to the number of vlans that need to traverse that trunked port. This is achieved by using the "allowed vlan" parameter. This prevents unnecessary VLAN information being passed across the network and prevents an attack from hopping across the network from VLAN to VLAN.

4.13.4 Router ACLs

These should be considered for use on all routing devices to control network traffic, whether it is for management, production or test. The relevant LLD for the device configuration will identify precise information based but the network security policy to be applied is to use extended access lists which identify both source and destination addresses and TCP or UDP protocol number.

4.13.5 Network Device Lockdown - Cisco "Auto Secure"

All HNG-X Cisco devices should be baselined with this tool. It implements a "one touch" device lockdown process that enables a rapid implementation of security policies and procedures to ensure secure networking services whilst removing the overhead on individual command line entries. Many of the features are taken from the NSA regulations. Appendix B shows what is enabled and disabled.

N.B. This security tool may disable services that are required by some network management applications.

4.13.5.1.1NSA guidelines

Each network component should be configured with a baseline security configuration that is initially derived from the relevant recommended NSA (National Security Agency's) guidelines for router, switches, firewalls and operating systems. In adhering to the NSA's guidelines access to the HNG-X network can be controlled, attacks resisted, other network components protected, and the integrity and confidentiality of network traffic maintained. These guidelines can be used in conjunction with Cisco's "AutoSecure" feature.

4.13.5.1.2Device Operating System

All network devices should be deployed with the current version of software in order to mitigate the risk of known software bugs. Cisco devices in particular should use the General Deployment version of IOS, and ensure that secure protocols such as SSH and SSL are supported. As the IOS version regularly gets updated by Cisco this HLD does not expect to identify, at this point, the exact version of software that should be deployed. At time of system configuration the device software should be considered and upgraded in accordance with the network security management policies.

One recommendation is to ensure that the Cisco IOS used has a cryptographic image. This would allow specific IOS security controls to be applied rapidly at any given time.

POL00398165

4.14 Securing, Deploying and Supporting HNG-X Network Devices

4.14.1 Baseline Device Configurations

As outlined at above the devices deployed must be configured with a mininum security baseline configuration. Engineers should apply this configuration prior to any deployment; any specific security enhancements, such as device ACLs, can then be configured afterwards. A list of the minimum security considerations, albeit not exhaustive, are shown in Appendix A.

4.14.1.1 Device configuration parameters/policy

The LLD for network devices will specify exact configuration, but an example of some security features that should be adhered to and applied are as follows:

- Interfaces not required for use to be administratively shutdown
- Network ports to have port security applied to them
- Speed and mode of ports to be defined i.e 100 full
- Passwords on devices to be encrypted
- Passwords to be 14 characters in length consisting of at least 3 upper, 3 lower and 3 numeric characters
- Remote access into devices limited to a certain number of management stations
- Banner notification on each device stating only authorised access is allowed
- Loopback interface is used for management purposes
- NTP enable with MD5 authentication
- VTP enabled in transparent mode
- Logging enabled and thresholds set
- SNMP v3 configured

A more comprehensive list of recommended parameters are shown in Appendix A

4.14.1.2 General alerts for Routers, Switches and Firewalls

Detecting potential network attacks and security violations can be mitigated by ensuring that the system is monitored and it has logging thresholds set to appropriate levels. All devices should have any access controls logged back to their associated logging server. Therefore, any traffic that has been denied can be identified and assessed to see if it is part of a determined, concerted attack on the network. This will provide evidence should the network security require enhancing.

- Firewalls and Routers - Log denied and accepted packets
- All devices - Log logon access to devices via AAA
- All devices - SNMP alerts such as link up, link down, config changes

POL00398165

4.15 Network Routing

Dynamic and Static routing will be in use in the LAN and WAN .Security constraints/or enhancements will be considered.

- Use of Static Routes as primary source of routing notification
- Use of "Passive Interface" to prevent unnecessary routing protocol advertisements.
- A Need for Routing Protocol Authentication –OSPF/BGP MD5 option
- Use of VRF as mechanism to hold separate routing table instances

4.15.1 Secure LAN Routing

The IGP routing protocol within the LAN is OSPF.

4.15.1.1 OSPF Routing Protocol Authentication

OSPF will be configured to used MD5 (Type 2) Authentication which uses MD5 cryptographic passwords. This will allow all OSPF neighbours to authenticate each other so that they can exchange routing update information in a secure manner.

The obvious security benefit is that it prevents a rogue device from potentially joining the OSPF routing domain as a neighbour with the intention of injecting false routes.

There is a security assumption made here that the password for MD5 authentication has not been compromised by any other breach.

4.15.2 Secure WAN Routing

WAN Routing is provided by C+W and is explained within the WAN HLD (DES/NET/HLD/0009). In terms of network security for HNG-X it is deemed secure for the following reasons:

- A MPLS VPN tunnel service is provided by C+W between remote sites and the DataCentres
- VRF-lite is configured on the CE routers and therefore separate instances of routing tables are maintained for each network.
- Risk of route leakage is low as separate VRF's are maintained for each VPN.
- IPSEC tunnels are provided by HNG-X between remote sites and the DataCentres via the 2811 Handoff Routers which offer the following security benefits:
    - C+W are unable to see HNG-X traffic
    - HNG-X have control of the IPSEC routing across the WAN
    - Termination of IPSEC tunnels are on HNG-X managed routers and therefore only HNG-X has the capability to configure.

With regards to further IPSEC information and parameters refer to IPSEC section at 4.5.4

4.16 Network Management Tools

Ciscoworks and Cisco Security Manager (CSM) are the applications that will be used to securely configure the network devices including firewalls and to undertake network diagnostics.

POL00398165

4.16.1 CiscoWorks

Installed within the Management LAN CiscoWorks LMS will support Cisco devices and apply security policies in terms of port security, IOS levels and configuration files. It will also be the destination server for device SNMP traps and syslogs.

By using this Management device to manage the routers and switches deployed across the HNG-X network, a strict control policy can be enforced. Support staff logon and authentication is used as any other server access, and all changes on the network are audited.

4.16.2 Cisco Security Manager

This tool will manage firewalls and ASAs and other security devices such as IOS routers which includes IPSEC VPNs. As with CiscoWorks, it provides centralised, auditable management, and minimises the security risk of changes being implemented on a firewall undetected. Again, access control to the server will be via the same process as other server logon.

This application will administer consistent firewall policies using the policy view feature of the application.

Creation of the policies and their deployment to the ASAs and VPN applied routers will be managed from this server that is located within the Management Services LAN.

It uses a GUI that provides an easy method of configuring policies and associated services and protocols.

DN: More information is expected to be added once assessment of this product has been carrie d out

4.16.3 Network Data Retention and Archiving

DN : A Comment on policy for storage of network logs is required.

4.17 Device IOS and Config Management

Patching IOS and providing updates is fundamental to the security of the network. The IOS of all devices must be free of any known bugs. Therefore areas of concern that may impact the network security are:

- Software Patch to current IOS
- Full IOS Update
- Configuration Backup

In terms of network security any device upload/download will be carried by authorised personnel, at scheduled times, using the processes and tools defined within Service Management.

4.17.1 Patching to Current IOS/Full IOS Update

IOS updates and changes to IOS versions can only be authorised by the Network Security Management team. Any supplier initiated bug alert or vulnerability notification must initially be sent direct to this team to assess the impact.

POL00398165

If as part of the day to day network management activities or as a result of a penetration /vulnerability test, a bug or vulnerability is found within the network it is the responsibility of the Network Security Management team to manage the issue and action it appropriately. This assessment may include any of the following:

1. Approve an immediate/scheduled IOS fix as bug is already known to project and the fix has already been tested and approved for deployment.
2. Interrogate the relevant logs to gather more information.
3. Notify the product supplier of the issue (using the standard support route)
4. Escalate the issue within the organisation following the Project procedures

4.17.1.1 Supplier provided bug fix

Any bug fix provided by a supplier will need to be assessed prior to deployment. This should be carried out under the operational Change control procedure and must include an assessment by the network security management team that the fix is suitable for deployment. It should be mandated by the Network Security team that the fix is implemented before hand on a standalone rig and functionality tests carried out.

4.17.2 Configuration Backup

This activity will be undertaken by the HNG-X System or Network Management team. All backups will be activated by a Job Schedule, probably via CiscoWorks. This will therefore be an auditable event that can be monitored by the Network Security team.

This action needs to be controlled so that it is clear that any configuration files copied off the network devices is done so as part of an approved service management activity, and that there has been no breach of security.

As any logon process is authenticated an audit trail can be maintained.

4.18 Network Change Control

4.18.1 Verification of Change Control

Any change to network IOS or configuration files must be verified by Network Security. This should be done in 2 phases:

1. Assessment of any change is carried out and the change authorised by appropriate personnel.
2. An action is carried out to cross reference the actual deployed configuration file or IOS with the specified and previously authorised change control.

4.18.2 Periodic Network Configuration Checks

Periodic scanning of the network devices and their configuration files must be undertaken to maintain configuration consistency and integrity. CiscoWorks should be configured to facilitate this by

POL00398165

- running a regular job to compare archived device configurations files with the running and start up files on deployed Cisco devices
- being configured for regular PING sweeps , at suitable intervals.

4.19 Penetration/Vulnerability Testing

This should be done at certain points in implementation lifecycle.

This security test will be carried out at an early stage of system acceptance. Ongoing vulnerability monitoring will also be carried out that will ensure that the network devices and software configurations are current and bug free. Any new device that is introduced into the network that does not conform to configuration standards will be identified. This activity will come under Network Security Management control.

4.20 Use of Network Sniffers

These are deemed as an acceptable diagnostic tool subject to the network security team verifying their use and their use is controlled. The network sniffer will assist in the following areas:

- Development/test arena for analysing traffic and application port numbers
- Live Arena for providing diagnostics to support team.

In terms of control a dedicated port should be reserved for use of any network sniffer. This in turn can be configured for a specific VLAN but no other end device should ever be plugged into the designated switchport.

4.21 Remote Access for Support

Remote Support for the HNG-X will be via the following:

- RMGA workstations on RMGA LANs (RED LAN)
- Corporate workstations (Corporate LAN users, remote access via Corporate LAN, and all other non-RMGA LAN internal networks) via crossbeams at SDC

Security of this support will be via

- IPSEC VPNs configured on the 2811 Handoff routers
- the SAS servers located in the Support DMZ LAN

Figure 7 below (taken from DES/NET/HLD/0009 v0.5) highlights the remote access route

POL00398165

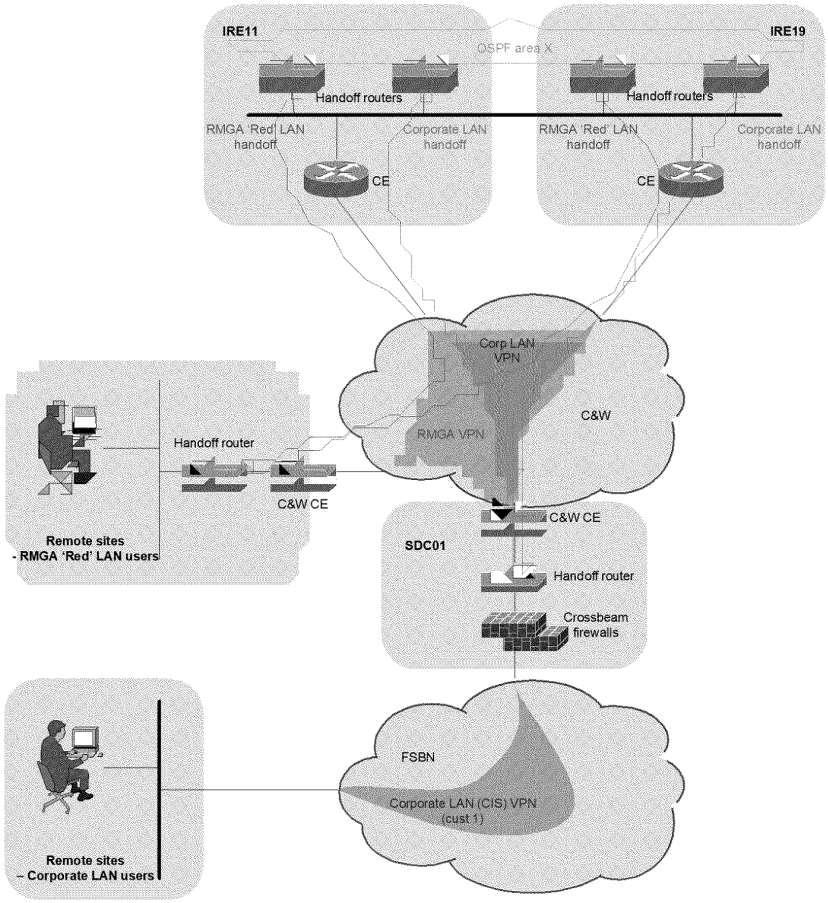

Figure 7 - Remote Access

4.22 Internet Access

DN: Need to discuss and understand further

This is required for software updates, antivirus updates and Post Office access to webserver for Broadband checker.

Current options:

- Via a C+W Internet VPN to be presented on Ire11/19 CE routers (Preferred)
- to utilise SDC01 Internet access point and then onwards to a C+W Internet VPN, then to the handoff routers in Datacentre (but would need a RMGA provided firewalls for inside /outside access)

The security concern is the obvious threats from the Internet. Security barrier i.e firewall and or ACLs will need to be applied

Figure 8 below (taken from DES/NET/HLD/0009 v0.5) highlights the Internet route via SDC01

POL00398165

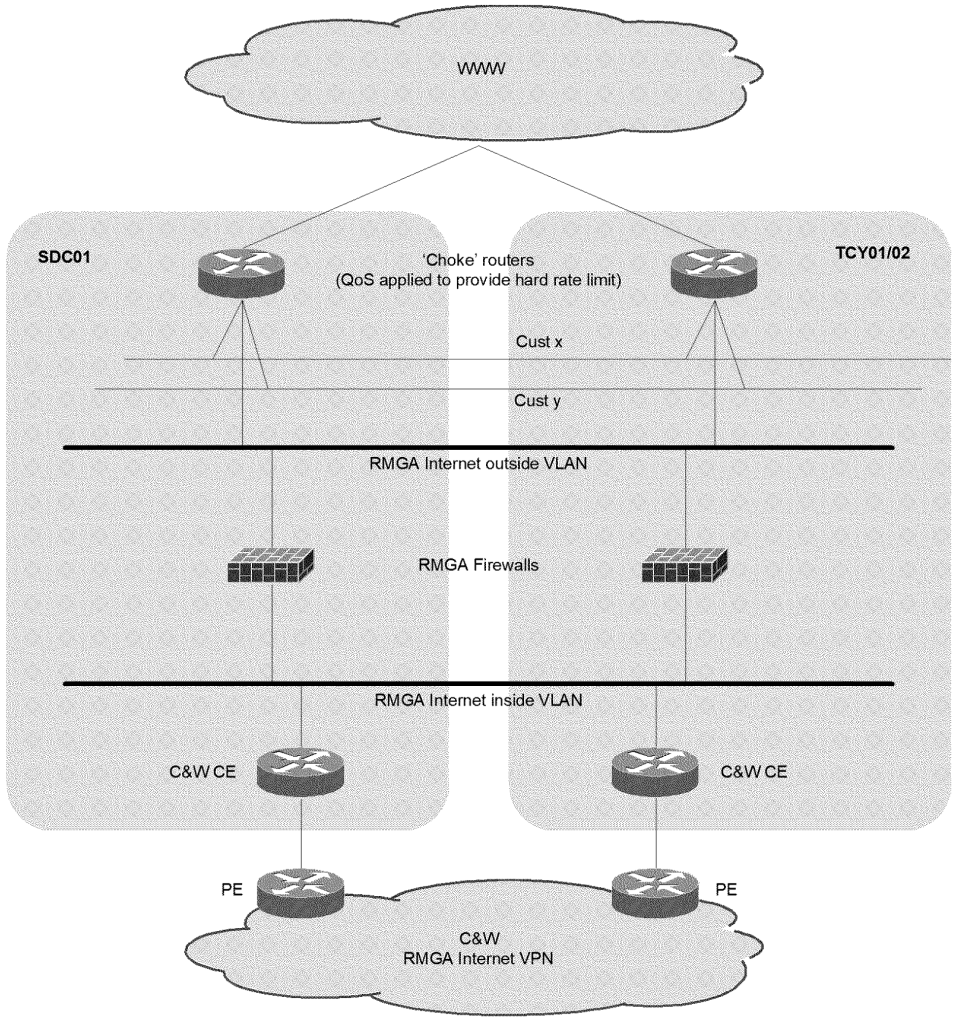

Figure 8 - Internet Access

4.23 Third Party Connections

DN: Need to understand and discuss further.

Interface rules for connecting into 3rd parties such as Corporate gateway, internet gateway, client LANs

4.24 Wireless WAN Security

Wireless WAN is secured by being logically separate part of the Orange network with IP A ddressing and authentication controlled by RMGA.

POL00398165

Branch routers connect to Orange for Live and Test and the traffic is kept logically separate. This is achieved by assigning SIM card for the environments to different APN's (access point name).Traffic from these APNs are sent across the Orange network in separate VPN's one for Test and one for Live.

4.25 ASDL –IPStream

ADSL service from Fujitsu called ConnectDSL. ConnectDSL will be reconfigured to use the BT SID (service identifier) so that the physical location can be identified to allow correct personalised info to router to be downloaded when it is being provisioned initially. This offers the security safeguard that the router is actually part of the HNG-X network.

4.26 General Device Security features

- Branch router uses MAC address security to restrict the devices that can connect to the network
- Branch router is locked using the following security features
    - Handling hard router resets- router goes back to default config that is security safe
    - The router firewall is configured to limit the WAN traffic to that explicitly allowed
    - Local management access ports including auxiliary, USB, management are blocked

POL00398165

A Device Configuration Security Parameters

A.1 Device Commands

The following should be considered for network devices. They can be used in conjunction with any other security measure such as Cisco AutoSecure:

Action	Command for Cisco device
GLOBAL command Disable unnecessary service	• *no service pad* • *no service ident* • *no service config* • *no service udp-small-servers* • *no service tcp-small-servers* • *no ip http server*[1] • *no ip source-route* • *no ip bootp server* • *no ip finger* • *no ip identd* • *no cdp run*
INTERFACE command Disable unnecessary service	• *no ip proxy-arp* • *no ip directed-broadcast* • *no icmp redirect* • *no icmp unreachable* • *no icmp mask-reply* • *no ip mop*
Logging	• *logging timestamps* • *logging console critical* • *logging buffered* • *logging trap debugging*

POL00398165

B.1 General Security Consideration for Devices

- Enable TACACS+ AAA. Two factor user authentication is via the TACACS+ server. The TACACS+ server offloads the username and password check to the Active Directory and Secure-ID servers.
- Ensure no default passwords are present in the device configuration
- Configure the rate threshold of allowable unsuccessful login attempts (*security authentication failure rate, login delay 2*). Enable logging messages for failed login attempts (*login on-failure log*).
- Secure Lines
    - Console, AUX, VTY, and TTY lines with passwords (see below for password specification)
    - Permit only access via SSH (*transport input SSH*, *transport output SSH*)
    - Specify timeouts to free lines after inactivity (*timeout 10*)
    - Last resort users are configured on all network devices to permit access with a known username and password should the TACACS+ service fail. The password is different for each network device; the username is constant. The last resort username and password should not function (allow login) if TACACS+ is operating normally. If the last resort password for a device is divulged to a 3rd party engineer, the password must be changed prior to re-introduction to the production service.
        - The last resort username has the following characteristics:
            - Case: mixed
            - First character: <alpha>
            - Subsequent characters: <alpha>|<numeric>
            - Minimum length: 9 characters (*security passwords min-length 9*)
        - The last resort password has the following characteristics:
            - Case: mixed
            - First character: <alpha>
            - Subsequent characters: <alpha>|<numeric>
            - Minimum length: 9 characters (*security passwords min-length 9*)
- SSH
    - Create a local Private / Public key set (1024 bits) for use by SSH / SCP
    - Restrict login times and attempts (*ip ssh timeout 10, ip ssh authentication-retries 3*)
- SNMPv3
    - SNMPv3 is supported in Cisco IOS Software Release 12.0(3)T and later.

POL00398165

- Disable SNMPv1 and SNMPv2.
- Define access lists to only allow connections from known management hosts
- Enable Authentication (password) and Privacy (encryption)
- Define a User the NMS systems will use to access devices
- Define groups for two classes of user access using the User Security Model (USM) v3
  - Read Only, view v1 default
  - Read Write, view v1 default
- Example:
  - *snmp-server engineID local 1111000000000000000000000*
  - *snmp-server user userthree groupthree v3 auth md5 user3passwd priv des56*
  - *snmp-server user userfour groupfour v3 auth md5 user4passwd priv des56*
  - *snmp-server group groupfour v3 priv*

- Access Lists
  - Remote access
    - Restrict connections via SSH, HTTPS to known management host IP addresses
  - Remote traffic filtering
    - No traffic with RFC1918 IP addresses should be allowed to enter or exit the HNG-X network.
    - Edge routers should block all RFC1918 traffic unless specifically agreed as part of a private interconnect defined in the technical interface specification.
- NTP
  - Enable NTP with MD5 authentication. All network devices should be stratum 2 devices synchronised with both NTP servers (one per data centre)
  - Network devices should make available an NTP service to devices on directly connected LANs. The device offering the service should be the LAN default gateway.
  - Configure an access list (*ntp access-group*) to only allow authorised NTP access
- Routing protocols
  - Keys should be defined to secure communication and prevent poisoning of routing updates
    - BGP
    - OSPF

POL00398165

C.1 Switch Configuration Security Considerations

- Macros should be configured and used to apply common security standards when the feature is available in 6500 switch IOS software.
- Ports
  - Unused ports to be placed in a dedicated VLAN – 999 – and shutdown
  - Auto-negotiation is disabled on all ports. The preferred mode is:
    - Speed: 1Gb
    - Duplex: Full
    - Trunking: Disabled
    - DTP: Disabled
    - Port security: Enabled (to mitigate against CAM table attacks)
    - PortFast: Enabled (for workstations / servers only)
    - 802.1x authentication and Network Admission Control: Disabled
    - Traffic Storm Control: Enabled (Broadcast control)
    - Unicast Reverse Path Forwarding: Enabled (Spoofed IP source addresses)
    - Control Plane Policing Control: Enabled (Filtering and Rate Limiting of traffic to the route processor; DoS prevention)
- VTP
  - VTP is enabled in transparent mode only. In this mode, the switch will transfer VTP advertisements between ports but will not act on them.
    - VTP passwords are used to authenticate VTP advertisements (for the future, if required, transparent mode does not generate or receive VTP advertisements)
    - There is one VTP domain per data centre.
    - VTP pruning is enabled.
    - Encapsulation negotiation is disabled.
    - Encapsulation is IEEE 802.1q
- VLANs
    - VLAN 1 is not to be used for production traffic (it is used solely for DTP, STP, UDLD etc) and should be pruned from all trunk links to avoid the nested VLAN (*VLAN Hopping*) attack.
    - A new default native VLAN should be chosen to be common across all data centre networks. The native VLAN is not used for production traffic to avoid the loss of CoS information.
    - VLANs 1 and 1002 through 1005 are reserved.
- Trunks
    - Trunks are restricted to explicitly permit allowed VLANs. The default is to permit no VLANs.

POL00398165

- Private VLANs are configured to mitigate against ARP attacks.
- VMPS is disabled.
- DTP is disabled.
- UDLD is enabled.

- ACLs
  - Layer 2 VACLs are used.
- STP
  - PVST+ is the STP (PVST+ includes BPDU Guard and Root Guard).
  - One core and one access switch at each data centre is biased to be the root switch.
  - Uplink Fast and Backbone Fast are enabled
  - Loop Guard is enabled
- ARP
  - Dynamic ARP Inspection and IP Source Guard are disabled as DHCP is not used.

POL00398165

B Cisco Auto Secure

Cisco Auto Secure performs the following functions:

ACTION	Protocol/Service Disabled
Disables the following **Global** Services	Finger, PAD, Small servers, Bootp, HTTP service, Identification service, CDP, NTP, Source Routing
Disables the following **Interface** services	ICMP, Proxy-Arp, Directed Broadcast, MOP service, ICMP unreachables, ICMP mask reply messages,
ACTION	**Protocol/Service Enabled**
Enables the following Global Services	Password-encryption service, Tuning of scheduler interval/allocation, TCP synwait-time, TCP-keepalives-in and TCP-keepalives-out, SPD configuration, no ip unreachable for null 0
Logging for security	Sequence numbers and timestamps, console log, log buffered size, interactive to configure the logging server address
Secures access to router	Checks for banner and provides facility to add text to automatically configure: • Login and password • Transport input and output • Exec timeout • Local AAA • SSH timeout and ssh minimum retries • Enable SSH or SCP for access and file transfer to/from router • Disables SNMP if not being used
Secures the Forwarding Plane	Enables CEF when available, anti-spoofing, blocks all IANA reserved IP address blocks, installs a default route to NULL 0 if a default route is not being used, configures TCP intercept for connection time-out if TCP intercept feature is available and user is interested, enables netflow on software forwarding platforms

POL00398165

C Traffic Flows and Firewall Rule Sets

D.1 Network Management

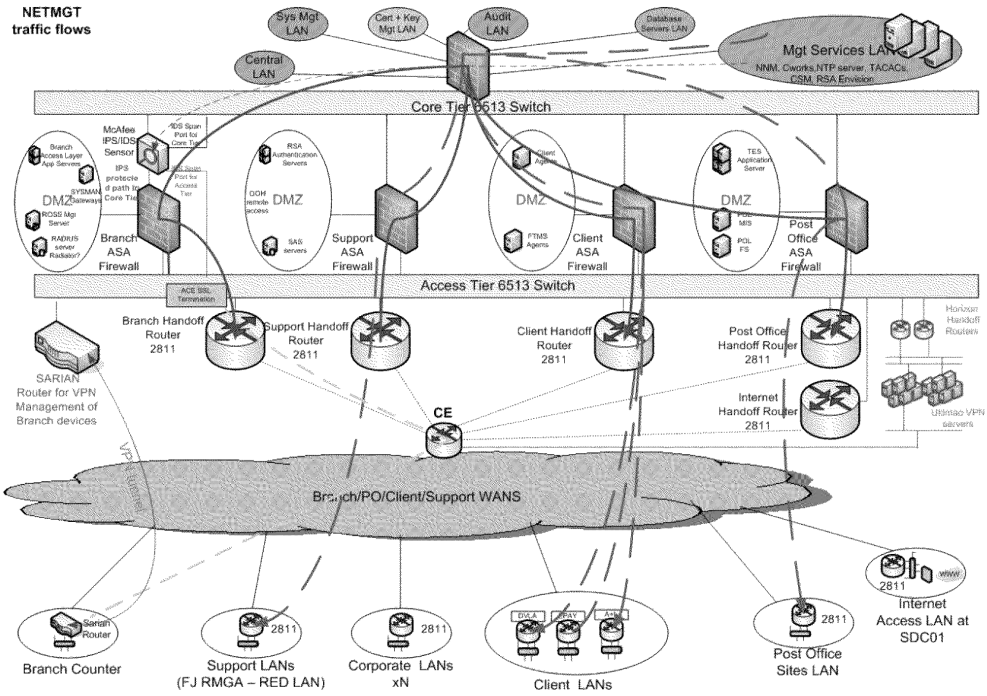

Figure 9 – Network Management Flows

Source	Destination	Protocol	Action	Comment
Management Services LAN	Remote LANs (Support, Corporate, Client, Post Office, Internet Access LAN)	SNMP (161/UDP) TFTP (69/UDP) SSH/SCP (22/TCP) TACACS+ (49/TCP) NTP (123/UDP) ICMP (TYPE 0,3,5,8 AND 11)	Permit Permit Permit Permit Permit Permit	Management of network devices
Management Services LAN	Internal network devices (Core and Access 6513 switches, ASAs, McAfee IPS)	SNMP (161/UDP) TFTP (69/UDP) SSH/SCP (22/TCP) TACACS+ (49/TCP) NTP (123/UDP) ICMP (TYPE 0,3,5,8 AND 11)	Permit Permit Permit Permit Permit Permit	Management of network devices

Table 10 – Network Management Protocols

POL00398165

E.1 Central

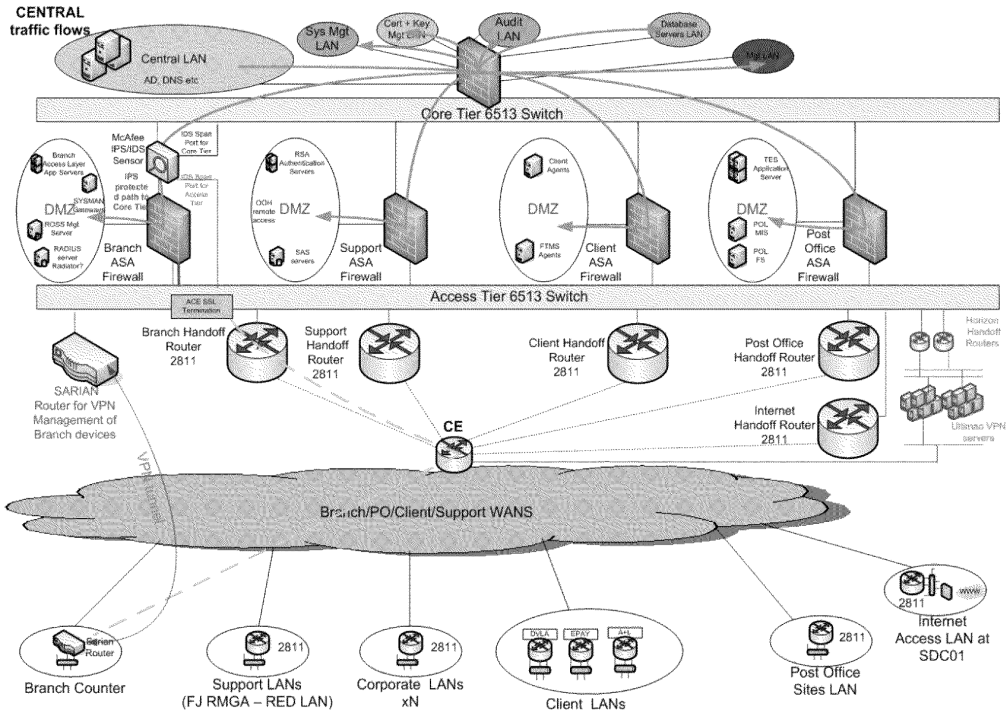

Figure 10 – Central Flows

Source	Destination	Protocol	Action	Comment
Central LAN servers	Servers on Internal LANs (Sys Mgt, Cert and Key Mgt , Audit, Database, Mgt Services)	SNMP (161/UDP) SYSLOG (514/UDP) Kerberos (88/TCP) Kerberos (88/UDP) DNS (53/UDP) DNS (53/TCP) SMB (445/TCP) ICMP (TYPE 0,3,5,8,11)	Permit Permit Permit Permit Permit Permit Permit Permit	Logging and Domain administration

Table 11 – Central Protocols

POL00398165

F.1 System Management

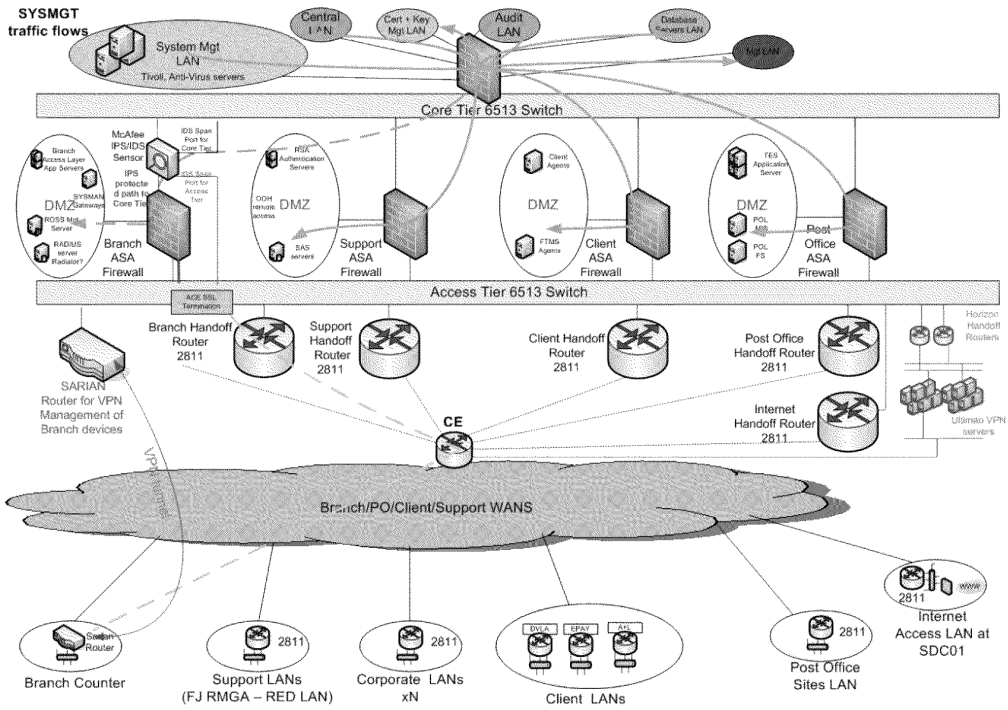

Figure 11 – System Management Flows

Source	Destination	Protocol	Action	Comment
System Mgt LAN servers	Servers on Internal LANs (Sys Mgt, Cert and Key Mgt , Audit, Database, Mgt Services) and Servers on DMZ LANs	TBA	Permit Permit Permit Permit Permit Permit Permit Permit	Anti-Virus agents, server system management

Table 12 – System Management Protocols

POL00398165

G.1 Certificate and Key Management

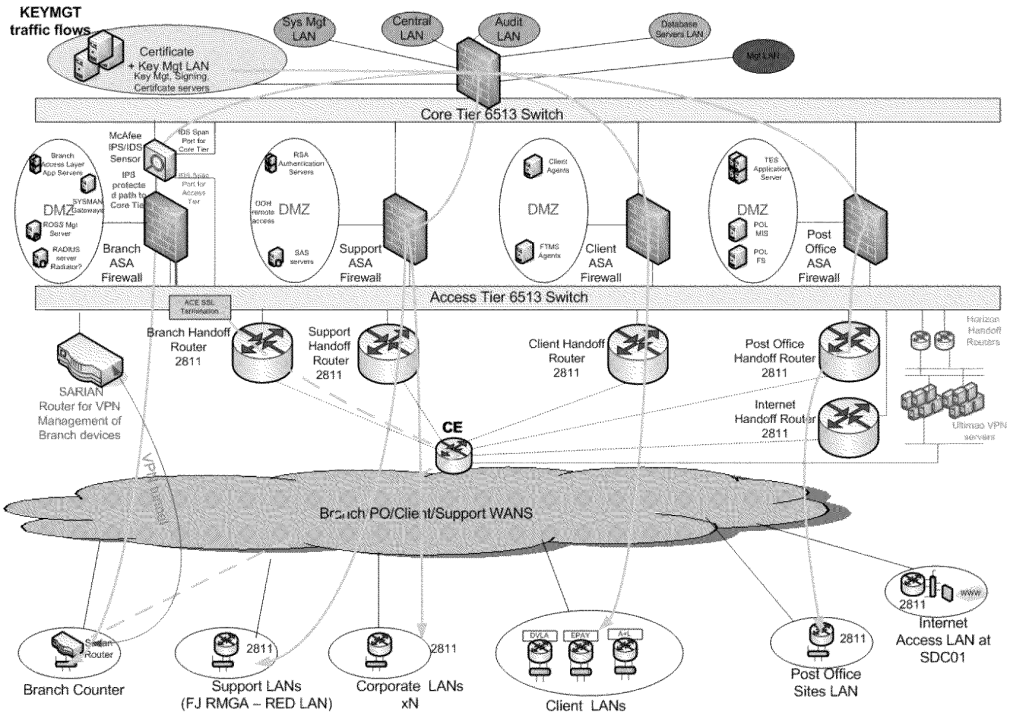

Figure 12 – Certificate and Key Management Flows

Source	Destination	Protocol	Action	Comment
Certificate and Key Management servers	Remote LANs and Internal Devices	TBA	Permit Permit Permit Permit Permit Permit Permit Permit	Certificate issuing and Key Management

Table 13 – Certificate and Key Management Protocols

POL00398165

H.1 Branch

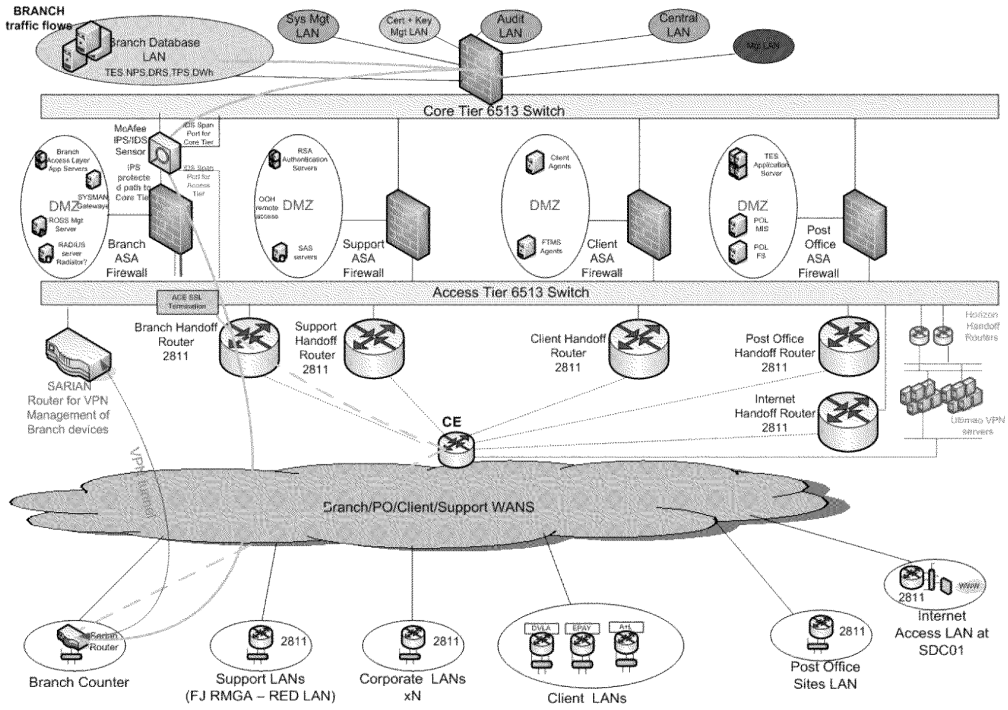

Figure 13 – Branch Flows

Source	Destination	Protocol	Action	Comment
Branch Database LAN	Branch Counters	TBA	Permit Permit Permit Permit Permit Permit Permit Permit	Database services for counters

Table 14 – Branch Protocols

POL00398165

I.1 Remote Access

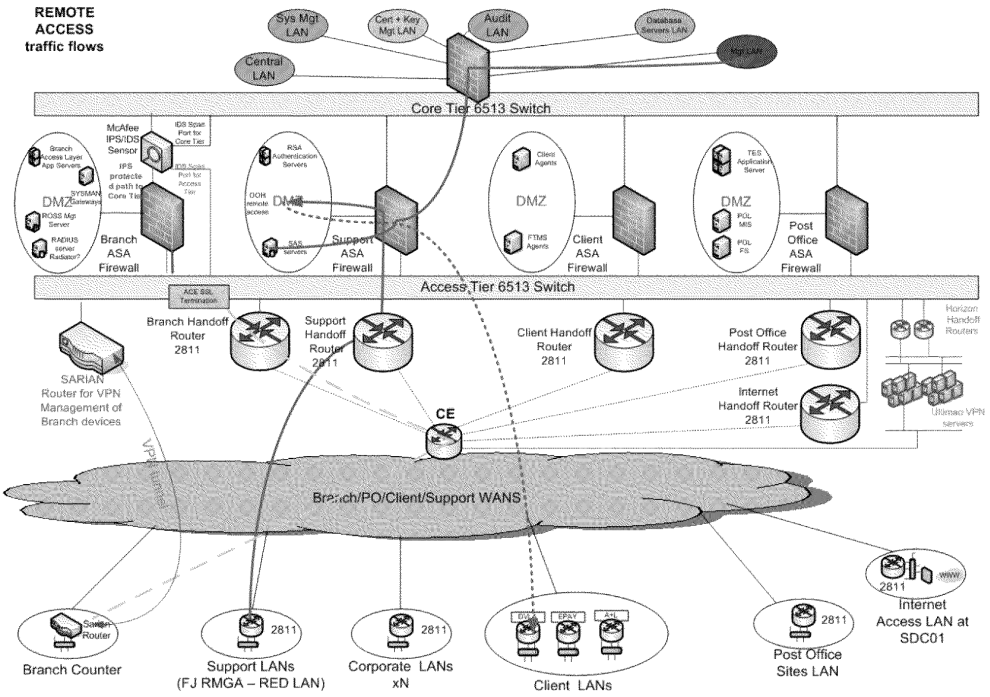

Figure 14 – Remote Access Flows

Source	Destination	Protocol	Action	Comment
Support LAN	Support DMZ – SAS servers	TBA	Permit	Remote access into SAS servers
Support LAN	Management Services LAN – McAfee Intrushield IPS Manager		Permit	Remote access for Management of MCAfee IPS/IDS Appliance

Table 15 – Remote Access Protocols

POL00398165

J.1 Audit

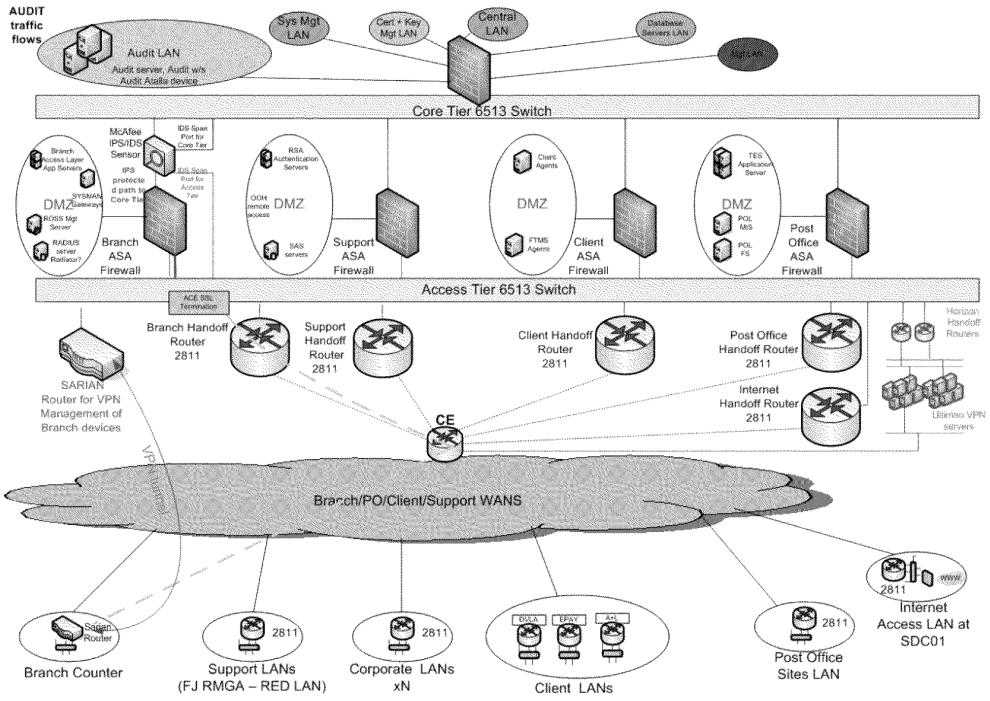

Figure 15 – Audit Flows

Source	Destination	Protocol	Action	Comment
Audit LAN	?	TBA	Permit	

Table 16 – Audit Protocols