Annals of Emerging Technologies in Computing (AETiC)
Vol. 2, No. 4, 2018

Long Article

Hardening CISCO Devices based on Cryptography and Security Protocols - Part II: Implementation and Evaluation

Faisal Waheed[1] and Maaruf Ali[2,*]

[1]Specialist Security Systems, BT Media and Broadcast, 60 Cleveland Street, London, W1T 4JZ, UK
faisalwaheed@live.co.uk
[2]Essex Pathways Dept., University of Essex, Wivenhnoe Park, Colchester, Essex, CO4 3SQ, UK
maaruf@ieee.org
*Correspondence: maaruf@ieee.org

Received: 1st September 2018; Accepted: 12th September 2018; Published: 1st October 2018

Abstract: This second part covers the implementation, testing, critical evaluation, conclusion and further study. It concentrates on the actual implementation details of hardening of network devices by referring to the hardware and software components, device operating system's features, management controls, access-list restrictions, operational configurations and critically making sure that the data and credentials are not stored or transferred in 'plaintext' over the network by detailed testing and evaluation. It investigates the commands used to enable cryptography and network protocols based on encryption, in order to meet the need for essential security requirements. Substantial work is devoted to the command line details and testing of a router based on *Cryptography and Security Protocols* in the border router. A step-by-step hardening approach is detailed using the commands used to secure the proposed network framework's border router. Encrypted services coupled with best practice configurations are explained and tested in an emulated environment. The use of protocol analysers, CISCO Configuration Professional's Audit and penetration testing tools corroborated the success of the project.

***Keywords:** AAA; ACL; APT; ASA; CEF; Control Plane; Cryptography; DDoS; DES; DMVPN; DMZ; DoS; Data Plane; EIGRP; GRE; Hardening CISCO Devices; HSRP; ICMP; IDS; IKE; IOS; IPS; IPSec; Management Plane; NAT; NHRP; OSFP; OSI; PSM; RADIUS; RIP; RIPv2; RSA; Security Protocols; SNMP; SNMPv3; SSH; SSHv2; SSL; TACACS; TCP/IP; VPN; VLAN*

---

1. Implementation

1.1 Overview

The hardening of routers and switches require the configuration of the management plane. This hardening process is carried out based on CISCO's NFP (Network Foundation Protection) i.e. upon the Management, Control and Data Planes. The main emphasis is on configuring the management and control planes as this is where the cryptographic keys and protective tools are applied followed by configuration of the security protocols such as DMVPN (Dynamic Multipoint Virtual Private

Network) and IPsec. Physical security is also applied at this level. The implementation phase of the project starts with restricting the remote login credentials and setting up access or privilege levels. These are explained as the implementation process is initiated. The passwords are encrypted using the IOS available features such as 'secret' or 'password-encrypt' services. The configurations become more detailed step-by-step.

1.1.1 Configuration Management Passwords

Line Console is the first part of a configuration where users are allowed or restricted access to the privilege mode. Privilege mode is part of the management plane where administrators can access the configurations of the network devices such as that of a router. This must be secured with an encrypted password which is performed later.

1.1.2 Line Console – (Console management port)

CISCO routers have ports enabled by default. Encrypted passwords must be set to block unauthorised access to these. The given configuration is the initial password setting commands for the first telnet session into the router:

```
Border-Router(config)#line con 0
Border-Router(config-line)#pass
Border-Router(config-line)#password cisco (Plain text password)
Border-Router(config-line)#login
Border-Router(config-line)#line con 0
Border-Router(config-line)#pass
Border-Router(config-line)#password
Border-Router(config-line)#password 7 cisco
```

1.1.3 Password Encryption – enable mode

The password has to be encrypted using 'password-encryption service':

```
Border-Router(config)#enable password cisco (plain text password)
Border-Router(config)#service password-encryption (Viganere encryption)
Border-Router(config)#enable secret cisco (encrypts password)
```

1.1.4 VTY Lines (Securing Telnet)

VTY is simply telnetted in CISCO terms, the initial configurations instruct users to allow users via Secure Shell (SSH) only:

```
Border.Crypto-Router(config-line)#access-class ALLOW-TELNET in
Border.Crypto-Router(config-line)#exec-timeout 6 0
Border.Crypto-Router(config-line)#password cryptovty
Border.Crypto-Router(config-line)#trans
Border.Crypto-Router(config-line)#transport in
Border.Crypto-Router(config-line)#transport input ssh
Border.Crypto-Router(config-line)#exit
```

1.1.5 Securing – Shutting down Auxiliary Port

The given configurations exclusively blocks access to the auxiliary port:

```
Border.Crypto-Router(config)#line aux 0
Border.Crypto-Router(config-line)#no password
Border.Crypto-Router(config-line)#transport input none
Border.Crypto-Router(config-line)#no exec-timeout
```

1.1.6 Enable and Encrypt the SSH Session (RSA)

The following commands enables and encrypts the SSH session:

```
Border.Crypto-Router(config)#ip domain-name Crypto-Router.com
Border.Crypto-Router(config)#ip ssh version 2
Border.Crypto-Router(config)#crypto key generate rsa
*Feb 26 15:12:08.563: %SSH-5-ENABLED: SSH 2.0 has been enabled
Border.Crypto-Router(config)#ip ssh maxstartups 3
Border.Crypto-Router(config)#ip ssh port 2101 rotary 2
Border.Crypto-Router(config)#ip ssh break-string SSH-Restrict
Border.Crypto-Router(config)#ip ssh authentication-retries 2
```

1.1.7 Encrypted Crypto Key certificate

The following commands sets up the asymmetric public-key cryptography encryption, as show in Fig. 1, below:

```
Border-Router(config)#ip domain-name Border-Router
Border-Router(config)#ip ss
Border-Router(config)#ip ssh ver
Border-Router(config)#ip ssh version 2
Please create RSA keys to enable SSH.
Border-Router(config)#cry
Border-Router(config)#crypto ke
Border-Router(config)#crypto key ge
Border-Router(config)#crypto key generate rsa
The name for the keys will be: Border-Router.Border-Router
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

Border-Router(config)#
Border-Router(config)#
*Feb 25 14:03:37.115: %SSH-5-ENABLED: SSH 2.0 has been enabled
```

Figure 1. Asymmetric public-key cryptography encryption using RSA.

The encrypted crypto key certificate information is shown below in Fig. 2:

```
Crypto PKI encrypted passwords:
username faisal secret 5 $1$aQWr$FqmZulgv6/2eGXH5tngDV/
crypto pki trustpoint TP-self-signed-4279256517
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-4279256517
revocation-check none
rsakeypair TP-self-signed-4279256517
```

Figure 2. Encrypted Crypto Key Certificate.

1.1.8 Enabling Secure HTTP/HTTPS service

The given configurations enable Hyper Text Transfer Protocol (HTTP) implemented for local telnet and directed to use the local encrypted password services set previously:

```
Enable Secure http service
Border-Router(config)#ip http secure-server
Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Feb 25 14:25:22.423: %PKI-4-NOAUTOSAVE: Configuration was modified
Border-Router(config)#login local
Border-Router(config)#ip http authentication local
```

1.1.9 Disabling vulnerable IOS services

The following commands disables vulnerable IOS services:

```
Border.Crypto-Router(config)#no cdp run
Border.Crypto-Router(config)#no ip unreachable
Border.Crypto-Router(config)#no ip unreachable
Border.Crypto-Router(config)#no ip finger
Border.Crypto-Router(config)#no service finger
Border.Crypto-Router(config)#no service tcp-small-servers
Border.Crypto-Router(config)#no service udp-small-servers
Border.Crypto-Router(config)#no ip bootp server
Border.Crypto-Router(config)#no ip reply-mask
```

1.1.10 Setting up Privilege Levels

The privilege level plays an important role in securing the management plane. Different privilege levels are assigned to different administrators from the top '15' to the least privilege level '1':

```
Border-Router#conf t
Border-Router(config)#enable secret level 15 0 fasifas9
Border-Router(config)#enable secret level 4 0 passlevel4
Border-Router(config)#privilege exec level 4 ping
```

1.1.10.1 Encrypted Passwords:

The following output verify the encrypted passwords set above.

```
username faisal secret 5 $1$aQWr$FqmZulgv6/2eGXH5tngDV/
enable secret level 4 5 $1$I8jB$2C86vTDV.U.hn99qfezXR.
enable secret 5 $1$WCAi$XyAFZxmOcy9lcc6Pzps6U/
```

1.1.11 Restricting Unauthorised Login Attempts

The services are set to a failure rate of five attempts after which the user is locked. This is to prevent a dictionary attack. This is shown in Fig. 3, below:

```
Border.Crypto-Router(config)#security authentication failure rate 5  log
Border.Crypto-Router(config)#aaa new-model
Border.Crypto-Router(config)#aaa local authentication attempts max-fail 3
Border.Crypto-Router(config)#aaa authentication login default local
Border.Crypto-Router(config)#login on-success
```

Figure 3. Configurations of max-attempts.

1.2 AAA Authentication

The Authorisation, Authentication and Accounting protocol play an important role in storing multi-router credentials. The protocol stores the user privileges in one of the servers; TACACS or RADIUS. AAA guarantees credential availability in times of a network outage.

1.2.1 Enabling AAA

The following commands enable AAA authentication:

```
Border-Router(config)#aaa new
Border-Router(config)#aaa new-model
Border-Router(config)#!! local data base
Border-Router(config)#aaa authentication login default local
```

1.2.2 Minimum Length password

The following commands enable a minimum password length of eight characters and tests it:

```
Border.Crypto-Router(config)#security passwords min-length 8
Border.Crypto-Router(config)#!! Prevent Brute force attack
Border.Crypto-Router(config)#aaa local authentication attempts max-fail 3
Border.Crypto-Router(config)#exit
Border.Crypto-Router.com#
Border.Crypto-Router(config)#username faisal privilege 15 secret 0 cisco
Testing: Password too short - must be at least 8 characters. Password
configuration failed
Border.Crypto-Router(config)#username faisal privilege 15 secret fasifas9
Border.Crypto-Router(config)#username user1 privilege 4 secret fasifas9
```

1.2.3 Configuring TACACS+ and RADIUS Server

Terminal Access Control Access Control System (TACACS) and Remote Authentication Dial-In User Service (RADIUS) are two main types of AAA protocols that are used to store the login credentials of administrators and networks management users in a central database, such as in an AAA server. However, we cannot rely on a single set of login (SSH) credentials stored locally on the router - as this can seriously compromise the security and availability of information stored in the permanent RAM also known as NVRAM. The AAA server is mainly deployed in a production (enterprise) environment where hundreds of routers are deployed, each sharing the same encrypted users credentials. These further secure routers as all the information are stored in a server. Administrators are directed to these servers for authentication and authorisation whenever they wish to login into a router. The servers checks for the provided username and password and allowed access based on the privilege level and authorised services.

1.2.4 TACACS+ implementation with Method-list

The Method-list provides a new flexible approach to programme the AAA protocol to grant access levels to administrators and users.

1.2.4.1 Authentication

The given configuration sets the local authentication level for login. The authentication level is given the name: 'FREE-BRID'. This simple configuration allows all type of login attempts, telnet, SSH and Aux port access for management purposes:

```
Border.Crypto-Router(config)#aaa authentication login FREE-BIRD none
Border.Crypto-Router(config-line)#login authentication FREE_BIRD
AAA: Warning authentication list "FREE_BIRD" is not defined for LOGIN.

Border.Crypto-Router(config-line)#login authentication FREE-BIRD
Border.Crypto-Router(config-line)#exit
```

1.2.4.2 Authorisation

AAA authorisation levels are created from highest privilege levels to the lowest level of '1'.

```
Border.Crypto-Router(config)#no cdp| advertise-v2
Border.Crypto-Router(config)#exit
Border.Crypto-Router(config)#aaa authorization commands 15 T15 group
tacacs+ local
Border.Crypto-Router(config)#aaa authorization commands 1 T1 group tacacs+
local
```

1.2.4.3 Accounting

Accounting deals with the logs of attempts and sessions that are forwarded to the AAA servers. This concludes the AAA server configurations.

```
Border.Crypto-Router(config)#aaa accounting commands 1 T-atg1 start-stop
group tacacs+
Border.Crypto-Router(config)#aaa accounting commands 15 T-atg15 start-stop
group tacacs+
```

Appropriate method lists have been applied to restrict the access of junior administrators to level 4. However, privilege level 15 has been given full access to management settings. This can sometimes create a security loophole as in many cases IT managers decide to allocate the highest level of access but restrict the administrators to view or run certain commands. This IOS-based security feature is known as 'Parser view'. Next, we are going to completely lockdown the management plane, followed by implementation of the Simple Network Management Protocol (SNMP).

1.2.5 Parser view (custom view – privilege level 15)

The Parser view feature is used to restrict administrators to a level where they can only view (show commands) authorised information. This feature not only provides security for within the administration team but limits unauthorised access to view command line configurations of the network. These set of commands are given below to implement this:

```
Border.Crypto-Router (config) #aaa new-model
Border.Crypto-Router#sh parser view
Current view is 'root'
Border.Crypto-Router (config) #parser view First-Line-Support
Border.Crypto-Router (config-view) #
Feb 29 15:30:36.811: %PARSER-6-VIEW_CREATED: view 'First-Line-Support'
Border.Crypto-Router (config-view) #secret fasifas9
Border.Crypto-Router (config-view) #commands exec include all
Border.Crypto-Router (config-view) #commands exec include all show
Border.Crypto-Router (config-view) #commands exec include all show ip
Border.Crypto-Router (config-view) #commands exec include show version
Border.Crypto-Router (config-view) #commands exec include show logout
Border.Crypto-Router (config-view #exit
Border.Crypto-Router (config) #username Faisal view First-Line-Support
privilege 15
Border.Crypto-Router (config) #aaa authentication login Telnet-Auth
Border.Crypto-Router (config) #aaa authentication login Telnet-othen local
Border.Crypto-Router (config) #aaa authorization exec Telnet-othor local
```

1.2.6 Disabling PAD – CDP – Source-route and TCP Keepalives

The CISCO Discovery Protocol (CDP) is a CISCO propriety service that allows routers to fetch detailed information about the neighbouring device's platform information. This includes ports they are connected to and details of the IOS. Disabling CDP restricts any unauthorised access to the key information of the routers. Packet assembler/disassembler (PAD) is also disabled for security, by the following commands:

```
Border.Crypto-Router(config)#no service pad from-xot
Border.Crypto-Router(config)#no service tcp-keepalives-in
Border.Crypto-Router(config)#no service tcp-keepalives-out
Border.Crypto-Router(config)#logging buffered
!! Given command disables Cisco Discovery Protocol (CDP)
Border.Crypto-Router(config)#no CDP run
Border.Crypto-Router(config)#no ip-source route
```

1.3 Telnet – VTY line – Access Control Lists

Although Secure Shell (SSH) remote sessions provide much better security, telnet is still widely used by the network administrators for remote management. Telnet sessions can be restricted to authorised users only. This is achieved by configuring the standard Access Control lists to permit required hosts and then apply the ACL to the line VTY (telnet) using the 'access-class' command.

1.3.1 ACL configuration

```
ip access-list standard ADMIN-ONLY
 permit 6.6.6.2 log
 permit 6.6.6.1 log
 deny   any log
```

1.3.2 Application to Telnet controls

```
line vty 0 3
 access-class ADMIN-ONLY in
```

1.4 CISCO Net flow (SNMP encrypted server)

Net flow is a CISCO proprietary protocol that is mainly designed to capture the interested traffic. The Net flow enabled server captures all the TCP and UDP packets. It works in conjunction with SNMP.

```
Border.Crypto-Router(config-if)#ip address 1.1.1.1 255.255.255.255
Border.Crypto-Router(config-if)#ip flow ingress
Border.Crypto-Router(config-if)#ip flow egress
Border.Crypto-Router(config-if)#int f1/1
Border.Crypto-Router(config-if)#ip flow ingress
Border.Crypto-Router(config-if)#ip flow egress
Border.Crypto-Router(config-if)#duplex auto
Border.Crypto-Router(config-if)#speed auto
Border.Crypto-Router(config)#ip forward-protocol nd
Border.Crypto-Router(config)#ip flow-export version 5
Border.Crypto-Router(config)#no ip http server
Border.Crypto-Router(config)#no ip http secure-server
Border.Crypto-Router(config)#snmp-server community public rw
```

The above commands set the ingress – 'incoming traffic' and egress 'outgoing traffic' on port FastEthernet 1/1. The command allows error reporting of internal and external traffic to be forwarded to the server 10.10.10.1 (MS loopback adapter) on the local host.

1.4.1 SNMP V3 (Encrypted – two key authentication)

SNMPv3 provides much better security for remote management as it offers multiple authentication key (encrypted – private key). The older IOS versions supported (Advanced Encryption Standard) but since DES (Data Encryption Standard - 56) provides more security, DES is implemented to stop eavesdropping. The configuration is shown in Fig. 4, below.

```
Border.Crypto-Router(config)#snmp-server view ALL-Area-ACCESS
1.3.6.1.2.1.2.2.1.1 included
Border.Crypto-Router(config)#snmp-server view INT-ACCESS ifEntry included
Border.Crypto-Router(config)#snmp-server  group  GROUP1  v3  priv  read  ALL-
ACCESS
Border.Crypto-Router(config)#snmp-server user Faisal GROUP1 v3
*Mar  2 13:33:48.111: Configuring snmpv3 USM user, persisting
snmpEngineBoots. Please Wait...
Border.Crypto-Router(config)#snmp-server user Faisal GROUP1 v3 auth SHA
Border.Crypto-Router(config)#$al GROUP1 v3 auth sha fasifas9 priv DES56
```

```
Border.Crypto-Router.com# sh run | inc snmp
snmp-server group GROUP1 v3 priv read ALL-ACCESS
snmp-server view ALL-ACCESS iso included
snmp-server view ALL-ACCESS ifIndex included
snmp-server view INT-ACCESS ifEntry included
snmp-server community public RW
```

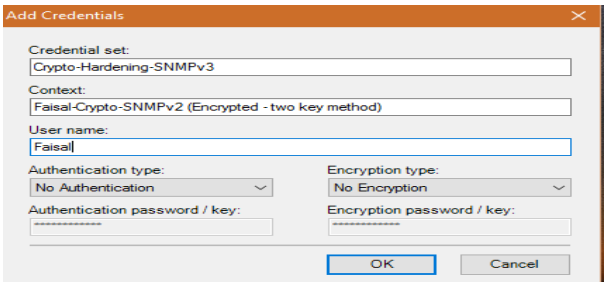

Figure 4. SNMPv3 configured with multi-encryption keys.

1.4.1.1 SNMPv3 Verification

Fig. 5, below verifies that SNMPv3 is active.

```
User name: user1
Engine ID: 123456789A
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: DES
Group-name: CRYPTO1

User name: Faisal
Engine ID: 800000090300CA0323880008
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: DES
Group-name: GROUP1
```

Figure 5. Multiple users showing SNMPv3 authentication as active.

1.4.2 Managing Engine Server

Solar winds engine server on local host 10.10.10.2 directing towards 'Border-Router' 10.10.10.1 is managed to record is shown to be successful in Figs. 6 and 7, below.

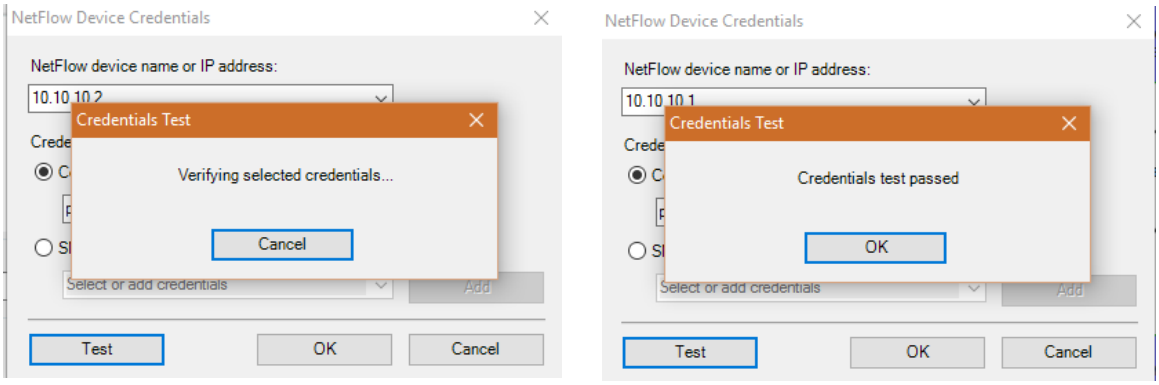

Figure 6. Management Server verification success.

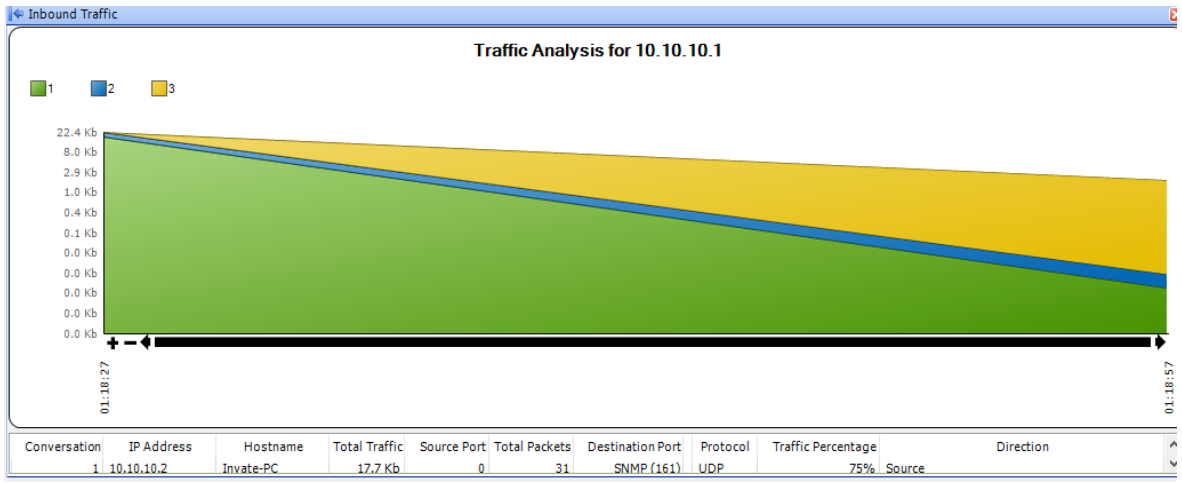

Figure 7. Inbound traffic graph confirming uninterrupted Net-flow (CISCO).

1.5 CCP Initial Audit checks

An interim audit report was issued next in order to check what services required further security. It clearly showed that the bulk of the services had been properly configured. However, a detailed analysis was carried out in the testing part of the project.

Services like CISCO Express forwarding and disabling Gratuitous arp are services that were successfully disabled. TCP and UDP small services along with Finger Services had been exclusively disabled. This closes doors for port scanning and TCP/UDP probe in the form of TCP SYN flood attack.

1.6 Securing the Data Plane

The data plane deals with routing and forwarding of traffic. Security protocols such as Access Control Lists (ACLs) are widely configured in routers, firewalls, and IDS. ACL is a must-have configuration that is applied to the interfaces (ports) in order to block any undesired or untrusted traffic in both external and internal environment. The focus remains on hardening the 'area border router' to block unauthorised traffic from outbound and inbound interface. There are two main types of access-list controls i.e. standard and extended. Standard access-lists are usually configured to block the source traffic only. Standard ACLs are not capable of blocking certain services such as Telnet, ICMP or SSH. Instead, it is capable of blocking a host or a whole network in some cases.

On the other hand extended access-lists can do much more as source and destination can be blocked based on the services criteria that needed to be 'permitted' or 'denied'. These are further

capable of filtering certain packets such as ICMP, IP and TCP and their respective services and ports numbers can also be blocked or allowed.

There are several other services that can be blocked in order to further harden network devices such as BPDU guard UNICAST RPF, Promiscuous Private VLAN (PVLAN), port security and STP/RSTP etc. Since we are mainly dealing with layer 3 routing device that runs on IOS image, certain services are not available within the layer 3 (C7200) router that we have deployed at the 'Network Door'.

1.6.1 Application of Extended-Named Access-lists Controls

1.6.1.1 Blocking internal traffic from any on-HTTP traffic (application in testing) is shown below:

```
Border.Crypto-Router(config)#ip access-list extended Block-Non-Http-Traffic
Border.Crypto-Router(config-ext-nacl)#permit tcp 20.20.20.1 0.0.0.255 eq www
Border.Crypto-Router(config-ext-nacl)#deny ip any any
```

1.6.1.2 Blocking Area router to SSH and Telnet (Unauthorised source)

This is shown below and confirmed as shown in Fig. 8, below.

```
Border.Crypto-Router(config)#ip access-list extended SSH-ONLY
Border.Crypto-Router(config-ext-nacl)# permit tcp 123.56.23.3 0.0.0.127
0.0.0.127 host 20.20.20.1 eq 22 (SSH port number)
Border.Crypto-Router(config-ext-nacl)# permit tcp 123.56.23.3 0.0.0.127
0.0.0.127 host 20.20.20.1 eq 23 (Telnet port number)
```

```
ip access-list extended Block-Non-Http-Traffic
 permit tcp 20.20.20.0 0.0.0.255 host 101.10.10.1 eq www
 deny   ip any any
ip access-list extended CRYPTO-BORDER-ROUTER
ip access-list extended SSH-ONLY
 permit tcp 123.56.23.0 0.0.0.127 host 20.20.20.1 eq 22
 permit tcp 123.56.23.0 0.0.0.127 host 20.20.20.1 eq telnet
```

Figure 8. Access-lists Controls allowing SSH traffic from 123.56.23.0 network only.

1.6.2 Blocking ICMP (ping) packets

These are implemented by the following commands and those in Fig. 9, below.

```
Border.Crypto-Router(config)#ip access-list extended  Block-Untrusted-Pings
Border.Crypto-Router(config-ext-nacl)#permit icmp host 20.20.20.0 any
Border.Crypto-Router(config-ext-nacl)#permit icmp host 192.168.10.0 any
Border.Crypto-Router(config-ext-nacl)#permit icmp host 192.168.20.0 any
Border.Crypto-Router(config-ext-nacl)#permit icmp host 192.168.30.0 any
Border.Crypto-Router(config-ext-nacl)#permit icmp host 192.168.40.0 any
```

Border.Crypto-Router (config) #ip access-list extended Block-Untrusted-Pings

```
ip access-list extended Block-Untrusted-Pings
 permit icmp host 20.20.20.0 any
 deny   ip any any
 permit icmp host 192.168.10.0 any
 permit icmp host 192.168.20.0 any
 permit icmp host 192.168.30.0 any
 permit icmp host 192.168.40.0 any
```

Figure 9. ACL blocking Untrusted pings from local networks.

1.7 Data Plane Security – IPsec and Cryptography

The tunnel is a logical connection between two devices such as end-to-end (border routers). IPsec creates a tunnel that encrypts all the packets and the other end decrypts it. Whether it is GRE or DMVPN, encryption provides secure (encrypted) data transfer in a virtual private network.

IPsec has two phases IKE phase 1 and IKE phase 2. IKE 1 tunnel is used for updates of hello packets and general exchange of tables. IKE phase 2 tunnel is mainly used for data transfer. IKE phase 2 is also known as a primary IPsec tunnel. In our case Site 1 Router encrypts the data and the other end decrypts it, from this point the Site 2 Router receives it in plaintext within its secured LAN environment.

IKE phase 1 negotiates hashing (MD5/SHA), Diffie-Helman (DH 1,2,5). Unlike AES (Asymmetric encryption) that requires a private key at each end. DH dynamically creates a shared crypto-key secret that is capable of securing a session against any middle attacks. We also need to specify the encryption types: DES, 3DES or AES, whilst configuring the router.

1.7.1 Topology Overview

The network topology of the simulation is given in Fig. 10, below.

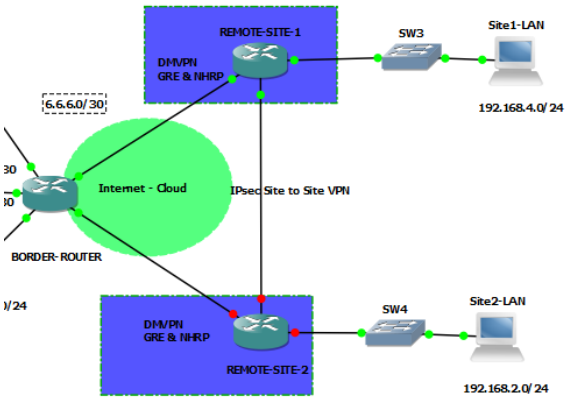

Figure 10. Topology showing overview of Border area router hardening area.

1.7.2 IPSEC Tunnel Phase 1 Configurations

IPsec phase 1 consists of setting up encryption and hash types, authentication, group (Diffie-Helman) and lifetime (age) of the tunnel.

1.7.2.1 Crypto Key Implementations

The following commands implement the crypto keys, as shown in Fig. 11.

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 86000
crypto isakmp key Faisal.crypto.project address 6.6.6.2
!
!
crypto ipsec transform-set Setting-Transform esp-3des esp-md5-hmac
!
crypto map CRYPTOMAP 10 ipsec-isakmp
 set peer 6.6.6.2
 set transform-set Setting-Transform
 match address CRYPTO-VPN-TRAFFIC
!
```

Figure 11. Configurations of IPsec tunnel phase 1.

1.7.2.2 Crypto Session Activate on Remote Site – 1

This is shown in Fig. 12, below.

```
Interface: GigabitEthernet1/0
Session status: UP-ACTIVE
Peer: 10.10.1.1 port 500
  IKE SA: local 10.10.1.2/500 remote 10.10.1.1/500 Active
  IPSEC FLOW: permit 1 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Figure 12. Session status of IPsec on port 500 showing as UP-Active.

1.7.2.3 Crypto key configurations

IPsec phase one requires a five-point configuration including that of: Data Encryption Service (DES), Message Digest 5 (MD5) and Diffie-Hellman (DH) group 2 coupled with pre-shared authentication that has to match on both the nodes (remote site 1 and remote site 2).

1.7.2.4 Crypto Session Active on Remote Site – 2

Internet Security Association and Key Management Protocol (ISAKMP) is standardised by RFC 2408 cryptographic keys exchange. ISAKMP defines the terms of the key exchange in a tunnel.

1.8 Securing the Control Plane with GRE and DMVPN

Generic Route Encapsulation (GRE), encapsulates the inside IP address to outside IP address. It creates a tunnel of IP addresses within public-private addresses. IPsec provides encryption whereas GRE provides an extra layer of encapsulated traffic. GRE is mainly deployed on top of IPsec (VPN) but unlike IPsec which is not capable of transferring the multicasts, GRE does. GRE tunnel provides additional security to the packets. Therefore, this was implemented in order to fully secure not only the routers but the respective traffic that it is sending or receiving.

1.8.1 Implementation of Cryptographic Protocols – GRE

The given configuration first creates a tunnel followed by the specified source and destination address. The tunnel (encapsulated) address has a private address (192.168.0.1) encapsulated in the private address (6.6.6.1) and destination address of 6.6.6.2.

1.8.1.1 Configuration on Border-Router

```
Border.Crypto-Router(config-if)#interface tunnel 121
Border.Crypto-Router(config-if)#tunnel source 6.6.6.1
Border.Crypto-Router(config-if)#tunnel destination 6.6.6.2
Border.Crypto-Router(config-if)#ip address 192.168.0.1 255.255.255.0
```

1.8.1.1.1 IP Table Entry – Show IP route

This is shown below in Fig. 13.

```
D    192.168.4.0/24 [90/297246976] via 192.168.0.2, 00:14:00, Tunnel121
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

Figure 13. Tunnel 121 route to 10.0.0.0/ 8 network appearing in IP table (Border-Router).

1.8.1.2 Configuration on Remote-Site-1

```
Remote-Site-1(config)#int tunnel 121
Remote-Site-1(config-if)#tunnel destination 6.6.6.1
Remote-Site-1(config-if)#ip address 192.168.0.2 255.255.255.0
```

1.8.1.2.1 IP Table Entry – Show IP Route

This is shown in Fig. 14.

```
D       10.0.0.0/8 is a summary, 00:15:23, Null0
C    192.168.0.0/24 is directly connected, Tunnel121
```

Figure 14. Tunnel 121 route to 10.0.0.0/ 8 network appearing in IP table (Site-1).

1.8.2 Implementation of Cryptographic Protocols – DMVPN

Implementation of Dynamic Multipoint Virtual Private Network (DMVPN) is very similar to Generic Route Encapsulation (GRE). But unlike GRE, DMVPN uses Next Hop Resolution Protocol (NHRP) to create multiple authentications, multicast and network ID configurations.

1.8.2.1 Border Router

The border router was configured next with these commands:

```
Border.Crypto-Router(config)#interface tunnel 131
Border.Crypto-Router(config-if)#tunnel source g 5/0
Border.Crypto-Router(config-if)#tunnel mode gre multipoint
Border.Crypto-Router(config-if)#tunnel key 1921
Border.Crypto-Router(config-if)#ip nhrp network-id 131
Border.Crypto-Router(config-if)#ip nhrp authentication fasifas9
Border.Crypto-Router(config-if)#ip nhrp map multicast dynamic
Border.Crypto-Router(config-if)#ip address 192.168.0.1 255.255.255.0
Border.Crypto-Router(config-if)#ip mtu 1400
Border.Crypto-Router(config-if)#ip tcp adjust-mss 1360
```

1.8.2.2 Router Site 1

The router site 1 was configured next with these commands:

```
Remote-Site-1(config)# interface tunnel 131
Remote-Site-1(config-if)#tunnel source g 2/0
Remote-Site-1(config-if)#tunnel mode gre multipoint
Remote-Site-1(config-if)#tunnel key 1921
Remote-Site-1(config-if)#ip nhrp network-id 131
Remote-Site-1(config-if)#ip nhrp authentication fasifas9
Remote-Site-1(config-if)#ip nhrp map multicast dynamic
Remote-Site-1(config-if)#ip nhrp nhs 192.168.0.1
Remote-Site-1(config-if)#ip nhrp map 192.168.0.1 6.6.6.1
Remote-Site-1(config-if)#ip nhrp map multicast 6.6.6.1
Remote-Site-1(config-if)#ip address 192.168.0.2 255.255.255.0
Remote-Site-1(config-if)#ip mtu 1400
Remote-Site-1(config-if)#ip tcp adjust-mss 1360
```

2 Testing

2.1 Overview

Next in-depth testing of implementation of encryption, keys, protocols and tunnelling methods used to harden the system were carried out. Analysis of the telnet session revealed the clear text password. The test also confirmed that Telnet was disabled and that Secure Shell (SSH) crypto keys were generated using RSA. Verification of SSH sessions also showed their statuses with multi-encryption keys – SHA and AES by packet analysis. SSH version 2.0 was secured with multi-level encryption keys including Advanced Encryption Standard (AES), Secure Hash Algorithm and Hash Message Authentication Code (HMAC). Observation of the TCP streams also verified this. The Telnet ACL was also verified to limit access. This included the login authorization and the allowed IP address (Access). The denied IP address (Access) was also tested. AAA Access level testing was carried out using a 'Free-Bird' method list with administrator rights using AAA debug. Debug also verified that 'FREE-BIRD' all-access login was authenticated by AAA.

Accounting side of AAA protocol kept a log of all the login activities sent to the server, RADIUS or TACACS+. The parser views were verified using sh privilege that showed that 'views' were created for privilege level 15 (root - all access) to privilege level 4 where restricted access is given to the administrator. SNMPv3 Stream content showed encrypted data at all ports as expected. The ingress and egress traffic were also confirmed to be encrypted by SNMPv3 with private key. Debug also confirmed SNMP (UDP) packets were being received at the Border Router. The restricted views were also verified.

2.2 EIGRP Secured Authentication

CISCO's proprietary Enhanced Interior Gateway Routing Protocol (EIGRP) is configured to automate routing entries. EIGRP uses 'Hello' packets to authenticate neighbour relationship. It is considered as one of the secured cryptographic protocol as it offers authentication mode of hash message authentication code (HMAC) and Secure Hash Algorithm (SHA 256) encryption decoupled with encryption password type as 'Message Digest' (MD5). EIGRP and Generic Route Encapsulation (GRE) makes a perfect match for 'inter' and intra-routing encryption.

2.3 Routing Protocol Debug

NHRP packets were authenticated with Routing Protocol over GRE tunnel. The IPSec Tunnel were also tested by encryption analysis using packet analyser. The Encapsulated Security Payload also revealed the encrypted data payload. Router console encryption was verified by sending pings to the destination LAN at site – 2. The GRE functioning was also tested using multicast address 224.0.0.10. Successful tunnel was found to have been created from source 6.6.6.2 to 6.6.6.1.

2.4 Testing NHRP and DMVPN – Next Hop Server

Here we verify Next Hop Resolution Protocol configurations that points encapsulated traffic to the next hop server (NHS) and successful pings confirm that. The 'Border Router' have been configured to act as a server in order to encapsulate all the dynamic multicast GRE traffic to other sites. The NHRP registration over the GRE tunnel was also checked.

2.5 Hot Standby Routing Protocol (HSRP)

Hot Standby Routing Protocol is CISCO proprietary usually implemented in homogeneous environments. HSRP is a legacy protocol developed after industry standard's First Hop Redundancy Protocol (FHRP). HSRP is implemented where redundant devices are deployed to offer users maximum network availability. HSRP works by setting up the same virtual IP address within the same subnet at gateway interfaces of redundant routers. One router act as an active router where most traffic is directed out to the outer world. In the case of a network outage, as soon as the active router goes down due to a faulty port or a problem with a link, the standby (backup) router takes over as the 'active router'. As a result, users do not notice any interruption.

2.5.1 Hot Standby test

Implementation of Hot Standby Routing Protocol (HSRP) is verified and tested to ensure the border link redundancy. The HSRP was active and the standby routers were found to have been

2.6 Reflexive Access-lists

Reflexive Access-lists was one of the advanced ACL types where the router can be hard coded as a firewall where the packets are inspected; denied or accepted entry based on the configurations. The main idea behind Reflexive Access-lists is that any traffic going out is remembered and logged into the system. It is like making a copy of a request going out, only that port number and source IP address will be allowed entry into the system, the rest of the packets will be dropped.

2.7 Context-Based Access-Control

CBAC uses firewall inspection rule to inspect the traffic on the way out so that the return traffic can bypass the ACL rule. Fig. 15, below shows the basic configuration of CBAC.

```
Border.Crypto-Router(config)#ip access-list extended Block
Border.Crypto-Router(config-ext-nacl)#deny
Border.Crypto-Router(config-ext-nacl)#deny ip an
Border.Crypto-Router(config-ext-nacl)#deny ip any an
Border.Crypto-Router(config-ext-nacl)#deny ip any any log
Border.Crypto-Router(config-ext-nacl)#int f2/0
Border.Crypto-Router(config-if)#ip acc
Border.Crypto-Router(config-if)#ip acces
Border.Crypto-Router(config-if)#ip access-group
Border.Crypto-Router(config-if)#ip access-group Block
```

Figure 15. Basic configurations of CBAC.

2.8 Pen Testing

Penetration Testing provides a real-time experience of 'ethical hacking' to evaluate vulnerabilities and exploits. Hackers require blueprint of a network in order to gain access to networks services. Gaining access to remote session either by Telnet (port 22) or SSH (port 23) is one the first steps for hackers to gain entry to a network. Since the project aims to stop hackers at their

first point of entry. Telnet and SSH ports are closed for any unauthorised access. This is tested by using the pen testing tools, i.e. Nmap, CISCO Global Exploit and CISCO Torch. The use of Nmap was able to discover vulnerable open ports. SYN flood attacks were also verified to have been successfully dealt with by observation of the destruction of ports from port 443.

2.9 Cross Checking by CCP Security Audit

CISCO Configuration Professional is an advanced and powerful Graphic user interface that is capable of verifying the most complex command line interface configurations. CCP is widely used by network engineers, professionals and for pen testers for auditing purposes. CCP has a built-in security audit feature that is capable of testing IOS based device's security configurations based on the location of the device within a network. CCP, however, does not verify any cryptography analysis as encryption requirements vary according to organisational security requirements. Implementation and testing of crypto-keys and the respective routing protocols have been successfully analysed using protocol analysers. The routers are hardened from the Management plane all the way to making sure that the data is transferred securely over the network (data plane). The project concluded with the router passing the final CCP audit of a router located at the 'border area'. This is shown in Fig. 16, below.

3. Project Analysis

3.1 Overview

This section provides the final analysis of the project in the form of evaluation as a result of advanced testing followed by conclusion and further work.

3.2 Critical Evaluation

The study was aimed at finding the current problem with networking devices, implementing a solution and later auditing the network in an emulated environment. Previous research and studies had been thoroughly analysed. The implementation of the router's functioning planes was carried out in an emulated environment. IOS was emulated in a virtual environment (hypervisors) due to the limited availability of hardware resources. CISCO framework was introduced within the topology based on best practices. CISCO's Adaptive Security Appliances (ASA) firewall was applied, however, the firewall did not contribute towards the interested part of the framework as the emphasis remained at hardening the 'Border Gateway Router' present at the Core layer of the CISCO design framework.

The background study provided a comprehensive understanding of encryption and hardening techniques used by the previous researchers. The network framework was implemented in the virtual environment, the emulated IOS hypervisors were given access to the real internet and local area network for enhanced real-time testing. Connecting the network environment to the external virtualized operating systems was the most challenging part.

Implementation of real-time encryption services from the management level to the data forwarding component (data plane) gave an insight into the importance of management services security. Hardcoded encryption techniques were applied, available within the CISCO IOS (C7200). Implementation phase revealed a number of vulnerabilities that were left running as default, which are summarised below:

- Line VTY (telnet) must be disabled as credentials are stored in clear text.
- Encryption plays an important role in management services.
- Secure Shell (SSH) access must be set as primary remote monitoring protocol.
- Special attention must be paid when applying Access control lists as a little compromise in configuration can cause a major outage.
- Password retries max-tries must be set to three to avoid dictionary attack.

- IPsec Virtual Private Network (VPN) alone does not fulfil the network security requirements.
- Encrypted routing protocols play a vital role in topology update.

Cisco CP - Security Audit Report Details

Router Details

Attribute	Value
Router Model	7206VXR
Image Name	unknown
IOS Version	12.4(13b)
Hostname	Border.Crypto-Router.com

Report Summary

No	Item Name	Status
1	Disable Finger Service	✔ Passed
2	Disable PAD Service	✔ Passed
3	Disable TCP small servers Service	✔ Passed
4	Disable UDP small servers Service	✔ Passed
5	Disable IP bootp server Service	✔ Passed
6	Disable IP ident Service	✔ Passed
7	Disable CDP	✔ Passed
8	Disable IP source route	✔ Passed
9	Enable Password encryption Service	✔ Passed
10	Enable TCP Keepalives for inbound telnet sessions	✔ Passed
11	Enable TCP Keepalives for outbound telnet sessions	✔ Passed
12	Enable Sequence Numbers and Time Stamps on Debugs	✔ Passed
13	Enable IP CEF	✔ Passed
14	Disable IP Gratuitous Arps	✔ Passed
15	Set Minimum Password length to less than 6 characters	✔ Passed
16	Set Authentication Failure Rate to less than 3 retries	✔ Passed
17	Set TCP Synwait time	✔ Passed
18	Set Banner	✔ Passed
19	Enable Logging	✔ Passed
20	Set Enable Secret Password	✔ Passed
21	Disable SNMP	✔ Passed
22	Set Scheduler Allocate	✔ Passed
23	Set Users	✔ Passed
24	Enable Telnet settings	✔ Passed
25	Enable NetFlow Monitoring	✔ Passed
26	Disable IP Redirects	✔ Passed
27	Disable IP Proxy Arp	✔ Passed
28	Disable IP Directed Broadcast	✔ Passed
29	Disable MOP service	✔ Passed
30	Disable IP Unreachables	✔ Passed
31	Disable IP Mask Reply	✔ Passed
32	Disable IP Unreachables on Null interface	✔ Passed
33	Enable Unicast RPF on all outside interfaces	✔ Passed
34	Set Access class on HTTP server service	✔ Passed
35	Enable SSH for access to the router	✔ Passed
36	Enable AAA	✔ Passed

Figure 16. Detailed list of services audited (passed).

The mentioned services and protocols are configured, enabled/disabled or applied to achieve the objectives.

During the testing phase, a number of vulnerabilities were found that revealed packets with clear-text passwords. Even after implementing the required services, encryption keys, protocols, and features, a number of exploits were found within the IOS. Network administrators must pay special attention when securing the networks. The evaluation is summarised below:

- Telnet services have to be manually disabled by using 'transport input SSH' using Line VTY command.
- Secure Shell cannot be practically implemented until the crypto key certificate is issued using RSA crypto-keys.
- Although 'secret' command does encrypt passwords but the login sessions can still be sniffed by protocol analysers. Therefore, the credentials must be manually encrypted using 'password-encryption' service.
- Parser views used to restrict administrators at management plane can be further programmed using 'method lists'.
- Disabling CISCO Discovery Protocol has several advantages but as it is disabled from global configuration mode, individual permissions cannot be granted. Therefore, the whole router disables the service if applied to the global configuration terminal.
- Secure HTTPs services must be enabled at the router global mode to provide encrypted services to terminal accessing websites securely over Secure Socket Layer (SSL).
- AAA server requirements are more relevant at the distribution layer within zone based Demilitarized Zone (DMZ) environments where several routers exist. However, AAA provides an extra layer of added security when used with local credentials.
- SNMPv2 is an improved version of Simple Network Management Protocol and still commonly implemented in corporate environments. SNMPv2 stores password in 'community strings' whereas SNMPv3 provides end-to-end encryption which must be implemented in a modern network.
- IPsec on its own does not provide encryption services alone, in fact, it works with other cryptographic protocols such as Dynamic Multipoint VPN and GRE coupled with NHRP.
- Limited penetration testing was not enough to fully test all the services.

To recapitulate, evaluation is totally based on the implementation in order to achieve the required objectives. Networking equipment hardening plays a decisive role in combatting network attacks: whether it is malicious insiders, Man in the middle, or remote hackers - encrypting services at all levels of networking devices is the only answer to reduce cyber-attacks.

4. Conclusion

Network Security is a wide-ranging issue that forces enterprises to spend billions of dollars to combat cyber-attacks. The most discussed term to combat cyber-attacks is 'cryptography'. Not only that it secures on-site networking devices but also protects remote monitoring and sessions that are critical to efficient management and performance of any network. Cryptography is one of the most demanded technology these days that provides a comprehensive solution to achieve end-to-end protection. Cryptography also guarantees more security to Confidentiality, Integrity and CIA triad. However, cryptography can be implemented at so many levels in networks. Therefore, it requires a greater amount of research in network security. On the otherhand implementation of encryption protocols unravels vulnerabilities in a network.

The study analysed the need of hardening devices, the role of cryptography in network security followed by implementation and testing of CISCO Internetwork Operating System. Based on detailed study of past research, objectives are met by in-depth testing with weaknesses evaluated to form a 'guide like' document for security administrators, network technicians and further researchers.

The research examined the real-time implementation of identified IOS features. The real devices are replaced with emulated operating systems implemented using Dynamips and hypervisors. This greatly reduced the simulation computing requirements. Techniques used in the study are most widely used in networks across the globe. The Management plane has been paid particular attention when closing all the doors for the hackers: Open ports, unencrypted passwords, vulnerable management services, ports, remote monitoring and other mal-configurations that give rise to a number of vulnerabilities exploited by hackers. Hence, leaving loops for the intruders to enter the system. Therefore, the management place is fully secured prior to application of the cryptography keys and security protocols.

The resulting hardened network device provided a safe, efficient, flexible and above all a cost effective solution to provide network security by making use of best practices to network configurations that are compiled in a document. The reality is that hardening network devices are such a broad topic, the study had to be narrowed down to the application of encrypted protocols in order conduct the study in the permitted time scale, budget and utilisation of available resources and budget.

CISCO devices outnumber deployment of networking devices across internetworks and the internet. Although CISCO IOS devices such as routers come with standard 'out of the box' guide but in terms of security, devices require a step-by-step hardening approach in order to fully secure the network based on requirements of an organisation.

Emulated CISCO IOS (C7200 – ver. 12.4) is secured based on the location of the router in a corporate network i.e. 'Border Router'. The term 'border router' is used in the study to refer to a router that is located at the edge of a network that acts as the first point of entry of any 'trusted' or 'untrusted' traffic. Although the study aimed at securing one distinct IOS at the border area, remote sites have also been secured by configuring multipoint encryption bundled with tunnelling and encapsulation provided by the implementation of GRE. The resulting router in the framework provides encryption between different 'border router' sites.

To sum up, all the objectives are successfully achieved, tested and audited by CISCO Configuration Professional (CCP) and pen testing tools such as Nmap, CISCO Global Exploit (CGE) and CISCO torch.

4.1 Further Study

The project titled 'Hardening CISCO IOS devices based on Cryptography and Security Protocols' provided a detailed analysis of encryption services available within IOS that is implemented and tested. However, the study lacked any analysis of data performance, efficiency or any potential jitter or interruption due to multiple encryption tunnelling or encapsulated packets. Network performance is one of the key business goals of any organisation. Cryptography techniques do provide multilevel protection, but the research indicate that the encryption and decryption process does slow down the data streams.

Further study on evaluation of network performance within cryptographic protocols will provide a detailed analysis of the impact on the actual traffic rate. It is also recommended that 'implementation of the cryptographic techniques with a step-by-step approach to measure network performance' need to be conducted on real hardware devices as this will provide more accurate results.

References

These are given in Part I, available at http://aetic.theiaer.org/archive/v2n3/p4.html.