

Long Article

Hardening CISCO Devices based on Cryptography and Security Protocols - Part One: Background Theory

Faisal Waheed¹ and Maaruf Ali^{2,*}

¹Specialist Security Systems, BT Media and Broadcast, London, UK
faisalwaheed@live.co.uk

²Int. Assoc. for Educators and Researchers (IAER), Kemp House, London, UK
maaruf@ieee.org

*Correspondence: maaruf@ieee.org

Received: 20th April, 2018; Accepted: 9th May, 2018; Published: 1st July, 2018

Abstract: Network Security is a vital part of any corporate and enterprise network. Network attacks greatly compromise not only the sensitive data of the consumers but also cause outages to these networks. Thus inadequately protected networks need to be “hardened”. The hardening of network devices refers to the hardware and software components, device operating system’s features, management controls, access-list restrictions, operational configurations and above all making sure that the data and credentials are not stored or transferred in ‘plaintext’ over the network. This article investigates the use of cryptography and network protocols based on encryption, to meet the need for essential security requirements. Use of non-secure protocols, underrating and misconfigurations of management protection are reasons behind network devices not properly being hardened; hence leaving vulnerabilities for the intruders. The gap identified after conducting intense search and review of past work is used as the foundation to present solutions. When performing cryptography techniques by encrypting packets using tunnelling and security protocols, management level credentials are encrypted. These include password encryption and exceptional analysis of the emulated IOS (Internetwork Operating System). Necessary testing is carried out to evaluate an acceptable level of protection of these devices. In a virtual testing environment, security flaws are found mainly in the emulated IOS. The discoveries does not depend on the hardware or chassis of a networking device. Since routers primarily rely on its Operating System (OS), attackers focus on manipulating the command line configuration before initiating an attack. Substantial work is devoted to implementation and testing of a router based on *Cryptography and Security Protocols* in the border router. This is deployed at the core layer and acts as the first point of entry of any trusted and untrusted traffic. A step-by-step hardening approach is adopted to secure the proposed network framework’s border router. Encrypted services coupled with best practice configurations are implemented 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. Introduction

1.1 Overview

Security has become more important as networks become indispensable and tools for breaking into networks become ubiquitous. Network design based on the implementation of optimal and secure routing protocols play a crucial part in securing these devices. A lapse in design management or underperforming routing protocols whether it is CISCO proprietary or industry standard, can cause major outages to the networks. Devices like switches and routers must be hardened to ensure maximum security for these devices.

'Hardening' is the process of securing a system and reducing its vulnerability from network attacks. Hardening a network device requires an in-depth knowledge of security features and protocols, available within the CISCO IOS.

When security breaches or network problems occur, the networks must recover quickly. This can only be achieved by having redundancy services or backup routers. The CISCO proprietary "Hot Standby Routing Protocol" (HSRP) plays an important rôle in restoring services in case of device fault discoverance.

The hardening of networking devices ultimately increases network performance. Furthermore, a top-down network design ensures a reliable network infrastructure. In the absence of these parameters, a network can experience outages and problems like: slow convergence times and decline in network bandwidth and performance - which can all jeopardise the running of a business. Therefore, there is an even greater need of the gateway border devices such as routers to be properly hardened, so that intruders can be prevented from entering the network. The project aims to harden border devices (routers) by implementing cryptographic protocols. These include the CISCO proprietary *Dynamic Multipoint Virtual Private Networks* (DMVPN) and the Generic Route Encapsulation (GRE) protocols.

The research simulation project is based on introducing a basic framework and top-down network configurations in order to harden the IOS devices, which is applicable to most organisations. However, the main objective is not just to introduce a framework or a design but also to provide a complete set of security solutions by configuring these devices against any external intrusions.

The rôle of cryptography, encryption techniques and cryptography protocol used to secure networks will also be discussed. These will be later implemented and tested as a part of a practical demonstration and findings from the tests. A detailed 'step-by-step' process of hardening the IOS based devices such as routers will be presented using real CISCO licenced IOS software, emulated to evaluate the findings.

The process may seem complex, as it requires knowledge of deep-down command line coding in order to harden the 'border router'. However, a thematic methodology has been adopted for a better understanding. Network and security administrators can refer to IOS configurations as a guide when deploying routers in a production environment at the enterprise level.

1.2 Hardening CISCO Devices

CISCO devices run on operating systems known as the Internetwork Operating System (IOS). Whereas network switches rely primarily on hardware rather than software, as they require fast frame and broadcast delivery to the nodes. Switches generally rely on 'Application Specific Integrated Circuits' (ASICs). ASICs are hard coded chips that are integrated within the chassis of the switch. CISCO devices support the running of multi-protocols and security protocols such as: Access Control List(s) (ACLs) that is based on packet filtering; Authorisation; IPsec; Open Shortest Path First (OSPF) and ASA (Adaptive Security Appliance) in the case of firewalls. A major challenge for network security administrators is how to select the appropriate security hardening measures, which can reduce the total cost while ensuring desirable network security.

The hardening process begins from the configuration of the management planes all the way to the data plane. The console remote login sessions along with login credentials and time-out session are encrypted. This is then followed by application of crypto-keys (i.e. MD5, SHA-1, SHA-256) and finally forwarding of the data based on ACLs.

Hardening and optimisation of devices work hand in hand as a neglect in one affects the performance of the other. Securing the devices means that loopholes or possible mitigation attack doors are protected by implementation of the available security features and protocols. A homogenous networking environment often uses proprietary protocols. For example, CISCO recommends Enhanced Interior Gateway Protocol (EIGRP) as its primary routing protocol.

Securing network devices by tuning of these protocols require identification of threats or vulnerabilities a network may experience. When analysing a network attack, considering these vulnerabilities in isolation is not sufficient. Networks can only be secure when these vulnerabilities are mitigated by investigating the loopholes within the security. These may include missing parameters from basic security i.e. lack of security configurations, leaving unused services on and bad choice of routing protocols. This results in a population of unused IP addresses in the routing table, which affects the network performance and makes it easy for intruders to take advantage of these flaws.

Routers are generally considered more at risk of attacks and therefore considered as the main gateway of intrusion, as these devices connect the public network to the private networks. Therefore, hardening and optimising routes as the primary device of security are crucial in achieving network security.

Most routing protocols are there for routing purposes only. It is a good idea to use more secure routing protocols. Routing protocols provide security through the use of peer authentication. The key factor in implementing any routing protocol is the likelihood of a router accepting invalid routing updates [1]. Application of more secure protocols, encrypted protocols such as IPsec, Dynamic Multipoint Virtual Point Network (DMVPN), Generic Routing Encapsulations (GRE) provides a secure environment for data transmission.

The implementation and testing phase of the project is carried out using GNS3, which is open source software that is capable of emulating real CISCO IOS routers. The emulated framework consists of routers, switches, ASA firewall, servers, and PCs. However, testing is only conducted at the 'border router' as that is the first point of entry of all trusted and untrusted traffic.

1.3 Article Overview

This first section is the introduction of the aims, objectives and rationale of the study. The second section, "Literature Review", mainly covers the theoretical part of the research and study. The third section is based on "Cryptography and Security", the basic concepts of security protocols. The importance of cryptography and the security protocols and their relevance is also discussed here. The fourth section deals with the concept of "Defence in Depth". Contents of this section are dedicated to the understanding of different layers of defence in depth. The focus of this study does not directly point towards discussing a different type of network attacks as emphasis remains on hardening IOS-based CISCO devices (routers). However, the most emerging, precarious and organised type of network type of network attack, Advance Persistent Threat (APT) is discussed briefly. The fifth section, "Methodology", provides a brief outlook of the framework and IOS image used to emulate the design. This includes the design, tools and software used. The sixth section deals with the "Implementation" of objectives based on detailed configurations of the router. The contents of the section mainly include configuration commands and verification of implemented services. The seventh section is dedicated to "Testing" of the implemented (configured) services, techniques, and protocols. The final section, eight, consists of findings, conclusion and recommendations and scope for further study.

2. Literature Review

2.1 Network Security and the OSI Model

Network Security is the backbone of information security because it secures the information passing through computers and devices. Security refers to software and hardware management, operational configurations, encryption, protocols, policies and satisfactory level of protection of these devices. In order to ensure the devices management, handling, infrastructure and design follows a standard pattern, the OSI model was designed to serve this purpose. The Open System Interconnection (OSI) model was created in 1970 in order to help vendors like CISCO adopt industry standards. However, in 1973 the TCP (Transmission Control Protocol) model was introduced and later divided into the TCP/IP protocol suite [2]. Today all the major networks around the world have adopted the TCP/IP model as the standard model. This was endorsed by the NSA (National Security Agency) in 2005, that most large companies use the TCP/IP protocol suite of IP addressing and security.

Behrouz [3] states that the initial design of the network layer had no security. However, today security is a big concern and cryptography and encrypted protocols are deployed at the network layer. The OSI model is mainly divided into two parts in terms of Host and Media layers, as shown in Fig. 1. The bulk of the security is applied in the 'Media Layers' that is made up of layers one to three of the OSI model. However, in many cases, the physical layer is not taken into the context of network security, where security devices like firewalls are deployed at the transport layer.

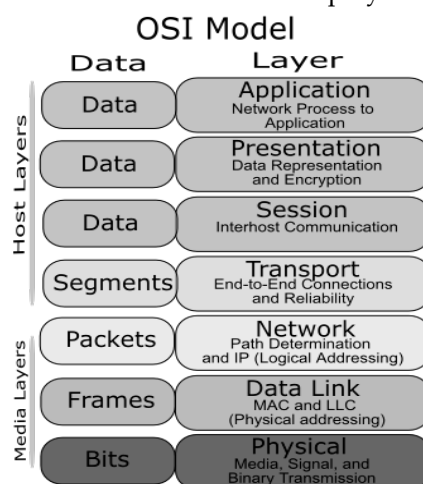


Figure 1. OSI Model Stack [4].

2.2 Security and Principle Goals

According to the NSA, routers play a strong rôle in securing networks. They operate on a distinct domain that is known as 'planes'. There are three distinct planes known as the Management, Control and Data planes, as shown in Fig. 2. In order to secure a router, the possible threats to each plane must be taken into consideration. Threats to the management and control planes mostly concern unauthorized access to the router or interference with router operation. Threats to the data plane usually concern violations of network security for the networks that the router supports. Basic hardening of routers includes physical security i.e. securing the ports, IOS security i.e. updated IOS software and finally configuration of a device using available security features and protocols.

2.2.1 Functional Planes

Much of the literature on router security divides it into three functional planes. This formula is mainly derived by CISCO and is known as Network Foundation Protection. Breaking the network into this layered plane infrastructure helps in planning and implementing the hardening of CISCO device security. According to Keith Baker [5], plane here means a function of each of these planes.

2.2.1.1 Management Plane

Network services running at the management plane allows the administrator to communicate with devices such as by the use of Secure Shell (SSH), telnet and Syslog. The management plane deals with the ability and function of managing devices. SSH encrypted services are often preferred for remote monitoring over telnet because it is secure. The question here may arise in the context of security as to what is the best of them all. Implementation of SSHv2 makes use of the Rivest, Shamir and Adleman (RSA) crypto-key certificate generated by CISCO IOS. In the case of brute force attacks, 'timeout' and 'max-tries' services are enabled. These locks down the users after three to five attempts. These can, however, be unlocked by the administrator later, if necessary.

2.2.1.2 Control Plane

This plane deals with device-to-device personal attention i.e. router updates, telnet requests etc. Here the CPU is involved, for example with: routing updates; traffic of the routes being directed to an IP address; authentication of routing protocol; policy and protection features. The control plane policing prevents all the bogus default routes. Policing limits numbering of router's session that is considered when dealing with inbound traffic like Internet Control Message Protocol (ICMP). The control plane deals with general thinking of the router and the common languages used to exchange critical information with other routers in the topology. The implementation of cryptography techniques at this level plays such an important rôle in ensuring the successful hardening of the router.

2.2.1.3 Data Plane

The data plane deals with the transit or forwarding of packets like frames. Examples would be the Internet Protocol Security (IPsec) and Secure Socket Layer (SSL) protocols operating in this plane. The Dynamic Multipoint Virtual Private Network (DMVPN) and Generic Route Encapsulation are CISCO proprietary protocols that provide further encapsulation and encryption/decryption when forwarding traffic.

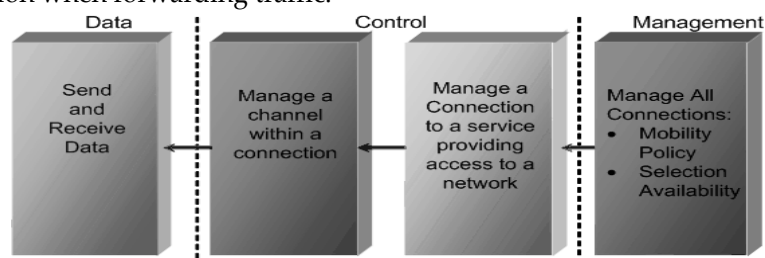


Figure 2. Operations at Different Planes of a Router [6].

2.3 Securing IP Network and Traffic Planes

Gregg [7] states that as IP networks continue to grow, so do the threats, therefore, no packet can be trusted. Man-made attacks include the purposeful misconfiguration of a router, poor network design and construction workers accidentally damaging say a fibre optic cable link. The trend of hacking has changed from script-kiddies to professional hackers. Amongst the many other tools, scripts and programming techniques, malicious worms and malware are injected into the network that result in an outage of networks. *Denial of Services* (DOS) attacks typically causes damage to the provider edge router (PE). Therefore, hardening border routers are crucial in achieving optimal network security.

Gregg [7] explains that the data plane contains, traffic generated by hosts, clients and servers. The control plane deals with routing protocols and most network attacks actually happen at Layer 3. Control packets, for example, are flooded by bogus packets which cause network outages and failures of network devices. The management plane is used for managing and monitoring of devices.

Keith Baker [5] mainly mentioned three planes but Gregg [7] introduced another plane which he referred to as the 'Service Plane'. He stated that it is the most important logical entity, as it deals with: *Network Address Translation* (NAT), Firewalls and *Quality of Service* QoS. It also deals with the more secure protocols such as: IPSEC, VPN (Virtual Private Network) and GRE etc. IPSEC provides high-speed encryption and decryption.

Network devices and interfaces include routers, switches, firewalls, IPS (Intrusion Prevention System), IDS (Intrusion Detection System) and load balancers etc. However, many CISCO routers and IOS devices provide built-in configurable security features that must be hardened.

2.4 Functional Architecture of a Router

A router is a hardware device that consists of CPU, RAM and ports for forwarding and routing purposes. The RAM stores the start-up files and configuration settings. These configurations include information about the routing protocols to be used, such as the: Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) etc. Routing protocols act as a common language between networking devices to share information like neighbouring configuration details, routing tables and the network topology view. A routing protocol is a combination of rules and procedures that let routers update critical information when a change happens in the network layout. Routers consists of:

- Routing tables that are stored in the RAM of the device. These are routes learned by the neighbour router. These are stored by the CISCO Express Forwarding (CEF) protocol. CEF is an advanced layer three switching technology. CEF is quite fast in making the forwarding table by transferring data to next hop routers. However, this routing information in the routing table is a primary honeypot for cyber attackers. Thus, routers being layer three devices are the most vulnerable devices for network attacks.
- The Console port that deals with the management of devices, setting up the Virtual Local Area Network (VLAN), assigning protocols, security and other tasks such as setting passwords etc.
- The Auxiliary port that is used for remote connectivity but functionality wise it is same as the console port as routers can be managed from a distance by a secure connection known as Secure Shell or Telnet.
- Routers are not, however, equipped with many Ethernet ports as they are mainly used for connectivity to an ISP (Internet Service Provider) or leased line provider.

Denial of Service (DOS) is a well-known type of attack that floods these routers with routing packets. However, CISCO IOS has optional features that can reduce the impact of flooding. The use of Access Control List (ACL) is a technique that allows only trusted networks to function whilst any spoofing or external flooding of packets from unlisted origins are dropped and blocked. ACLs match packets using source IP addresses. These ACLs are frequently used to protect a router's data plane (that is, to filter traffic traveling through a router). However, ACLs can also be used to help protect the management plane and the control plane [8].

2.5 Router Security Policy

According to Wallace [8] CISCO's routers security policy mainly address the following parameters:

- **Passwords:** passwords need to be encrypted.
- **Authentication:** remote management of the routers via telnet or SSH security is deployed by using authentication, authorisation and accounting AAA (Authentication, Authorising and Accounting) protocol using Terminal Access Controller Access-Control System (TACACS) and Remote Authentication Dial-In User Service (RADIUS) server. Banners are set here to prevent unauthorised access.
- **Access:** the preferred remote management tool SSH is preferred over Telnet due to its encrypted nature.

- **Services and Filtering:** certain ports are disabled for extended access and packets filtered using Access Control List as already discussed.
- **Routing Protocols:** using the most secure routing protocols.
- **Redundancy:** redundant devices are deployed in case of an attack to one router.

2.6 Routing and Network Security Protocols

The three main categories of routers that are deployed as Internet gateways (border router), corporate internal and B2B (business-to-business) must be hardened in order to prevent an organisation from both internal and external intrusions. Fig. 3. illustrates the critical gateway rôle of border routers.

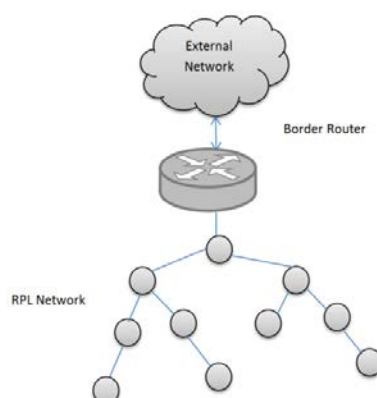


Figure 3. Border Router location between untrusted (external) and Routing Protocol for Low Power (RPL) Networks [10].

McGee [10], suggests that network security cannot be achieved by simply deploying a firewall. However, contrary to his work, Xiao-Feng *et al.*, [11] presented a mathematical framework and based on his findings, he was convinced that the essence of network security is intrusion detection systems and firewalls. The proposed model had both an external and internal firewall in order to mitigate attacks. Firewalls play an important rôle in the accomplishment of high-security levels. However, this is not the case in conventional networks, as the firewall is not capable of routing. An 'external router' defined in CISCO terms has to be deployed before the firewall. For this reason, hardening the border routers are recommended since they are the first point of direct exposure to the outside world in order to strengthen network security.

Even though CISCO devices come with necessary documentation, there is still a need for hardening these devices beyond their basic security configurations. For example, creating passwords in just plaintext is not a good practice. Using encrypted service in Secure Shell (SSH) in the management plane is a good practice.

Jankunaite *et al.*, [12], advises that VPN tunnelling techniques such as IP Security (IPsec) and other security protocols that provide header encryption should be used to secure the networks. The importance of securing border routers is stressed in his findings. Similarly, security protocols must be implemented at the Border Gateway Router (BDR) as suggested by CISCO - as these are the main routers that connect the corporate network to the outside world. These are the first point of entry for any external traffic to enter the internal network. Therefore, these protocols and hardening configuration will be applied at the implementation and testing phase of the project.

In contrast, Chen [13], discussed the limitations and risks involved in a less secure VPN. He is of the view that 'Tunnels' in a VPN are more complicated networks to configure and maintain. CISCO's proprietary protocols i.e. Generic Routing Encryption (GRE) is highly criticised as it may cause certain packets being dropped. Despite this criticism, the popularity of VPN and GRE remains, as they are still the commonly used protocols adopted by enterprise networks. Furthermore, he recommended a technique that is much more viable and secure in the current environment i.e. to

implement IPsec on top of GRE to establish a tunnel, make use of the Next Hop Redundancy Protocol (NHRP) to utilise Dynamic Multipoint VPN's functionality. Noting the compelling nature of this new evidence, a network based on the Dynamic Multipoint VPN will be simulated and then tested and the compared findings against the IPsec-VPN will be evaluated. Whilst configuring the devices, CISCO proprietary protocols such as EIGRP, GRE, NHRP and DMVPN are implemented due to their suitability of performing well within homogeneous network environments.

Priscilla [14] further suggests that it is a good practice to use *Secure Shell* SSH and disable telnet, as SSH uses secure password encryption cryptography. TACACS and *Authorisation, Authentication and Accounting* (AAA) can be used to manage a large number of login credentials. Priscilla [14] is convinced that in order to protect internal networks, it is important to protect internetworking devices such as routers and switches. Routing Protocol should authenticate the neighbour router's protocol. An example of protocols that provide encryption is Routing Information Protocol (RIPv2), Open Shortest Path First (OSPF), Internet Protocol Security (IPsec) and Dynamic Multipoint Virtual Private Network (DMVPN). VPN play an important rôle in remote connectivity required by the network administrators around the world. However, due to its limited encryption capability, researchers have suggested other 'more secure' protocols.

2.7 Rôle of Cryptography in Network Security

The Internet is a packet-switched network, the data packet pass through many routers before reaching its final destination. This means any unencrypted data can be easily read by any 'Man-in-the-Middle', thus compromising confidential information. Encryption is the 'practice of scrambling data' that could only be read by decryption devices with relevant keys. "*Cryptography*, a word with Greek origins, means "secret writing." However, the term is also used to denote a technique to scramble data into an unreadable form, so that only the authorised personnel have access to the secret data" [3]. Cryptography is referred to the **encryption** and **decryption** of IP packets, data and messages using secret keys. In networking, cryptography is used in the form of encrypted protocols and encryption keys in a different format such as Message Digest (MD5) and *Secure Hash Authentication* (SHA).

In a review of the literature Tat *et al.*, [15] made an effort to integrate cryptography techniques i.e. *Public-Key Security Model (PSM)* into *Simple Network Management Protocol SNMP*. The conclusion was based on the findings that use of SNMPv3 with PSM provides greater security with authentication, encryption and stronger cryptographic techniques. The management protocol is widely used in network infrastructure in order to monitor network performance and security. SNMP has gone through many revisions over the years. The latest version of SNMPv3 uses cryptography techniques.

SNMPv1 and SNMPv2 did not provide encryption, it is, however, important to note that many organisations are still using SNMPv2 due to its popularity and consistency within the monitoring side of security.

According to Nemati and Yang [15], the 'man in the middle attack' occurs when an anonymous entity is decrypting public keys. The sender and receiver are unaware of an intrusion and continue to transmit data as if they are talking to each other.

Bhaiji [17] suggested that device-hardening modules are one of the fundamental security models that should be configured to protect the network devices from any attacks. This according to Nemati and Yang [15] is only possible if cryptography keys are used. Brute force is a type of attack that generates random passwords in plaintext. Cryptography plays a very important rôle in securing the network devices, packets, and data. RSA crypto-keys are used in the process of hardening CISCO devices. The use of a Crypto Router is shown in Fig. 4.

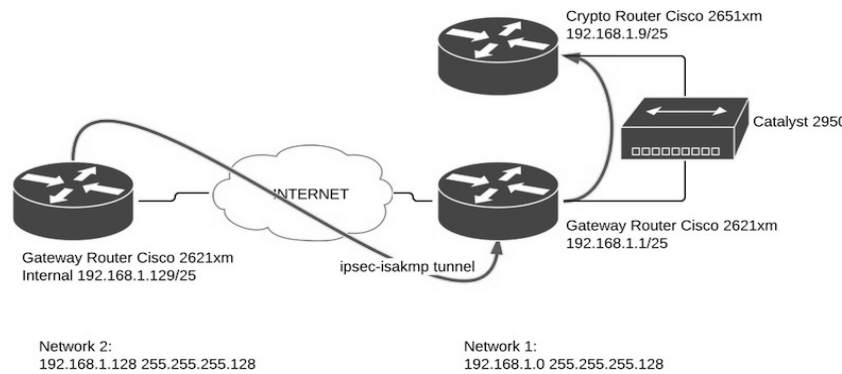


Figure 4. IPsec Tunnel Traffic Passing to Crypto Router [18].

For security, information that is to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity) and available to an authorized entity when it is needed (availability) can all be met by the use of cryptography.

In a review of the literature, Tat *et al.*, [15] made an effort to integrate cryptography techniques i.e. *Public-Key Security Model (PSM)* into *Simple Network Management Protocol SNMP*. The management protocol is widely used in network infrastructure in order to monitor network performance and security. SNMP has gone through many revisions over the years. The latest version of SNMPv3 uses cryptography techniques.

2.8 Related Work and Techniques

SANS Institute [19] released their 'step by step' security guide. The document was based on the required configurations for the security of CISCO routers followed by a similar document released by the National Security Agency (USA). These studies were very similar in nature as the available CISCO routers were discussed along with the rôle of encrypted and secure protocols such as *IP Security (IPsec)*. The importance of having 'banners' and security in different modes of the router management interface were researched. The research papers released however did not undergo any implementation or testing within a network framework.

According to Sheth and R. Thakker [20], their view is that a firewall configuration contains a large set of rules that are based on source and destination address. The actions are accepted or denied, meaning the transfer or dropping of the packets. This is confirmed by Baker [5] in his book, *CISCO Network Security*. Sheth and Thakker [20] further states that most vulnerabilities are detected as a result of misconfiguration of these firewalls, these also include routers. His comparative study was based on CISCO's ASA and Checkpoint Secure Platform (SPLAT). Based on TCP throughput, CISCO's Adaptive Security Appliance ASA firewall outclassed the SPLAT. Therefore the industry's leading firewall i.e. the ASA firewall will be implement in the proposed framework for the testing and auditing of the network. It is important, however, not to assume the applicability of the firewall in all cases. The Demilitarized Zone (DMZ) is part of an internal network that is a 'trusted' network, this may comprise of DMZ servers and workstations. However, due to the trusted nature of this zone, an intermediate level or security is expected and applied.

In an attempt to test vulnerabilities in CISCO IOS devices, Peine and Schwarz [21] implemented a tool, 'CROCODILE' in order to track router security. "Crocodile performed a semantic analysis of the configuration". It was geared towards the market leader in routing, CISCO. The tool was used to audit the basic user authentication and security checks. Due to its integration within the CISCO IOS, it raised many questions on the performance and security of CISCO devices. Defects were uncovered later as many critical services were potentially left running. That left a question mark within the testing environment as further research was needed. It can be seen from the above analysis that the most crucial service in network security is left running that ended the testing without any reasonable discovery or results.

Fengjiao Li [11] states CISCO IOS has serious security loops. According to the National Vulnerabilities Database, CISCO devices had 1807 vulnerabilities. Previous studies like

CROCODILE has worked for basic debugging but due to limited research testing on CISCO devices were still limited. Fengjiao Li [11] used a technique called ‘Fuzzing’ to detect potential vulnerabilities within the router. The router’s IOS were simulated by Dynamips, a tool that is capable of emulating CISCO IOS. The tool was very similar to GNS3, which will be used to emulate the CISCO IOS. The fuzzing testing process, however, experienced drawbacks. For instance CPU utilisation went to 99%, this had a negative impact on the study. The approach is very similar to Sheth and Thakker [20], who too failed in achieving the desired result.

‘Fuzzing’ is an inefficient technique to test a CISCO router for security loops. Injecting IOS with raw packets (scripts) is nothing but a test to check how well a router can perform when bombarded with random packets. However, it is to be noted that in order to test a router’s security, it first needs to be hardened by application of security protocols. Testing the devices afterwards seems like the most effective and appropriate approach in identifying its vulnerabilities. An overview of network security research is given in Table 1, below.

Table 1. Overview of Network Security Research.

Researchers	Techniques
Tat <i>et al.</i> , [15] made an effort to integrate cryptography.	Techniques used were integrating Public-Key Security Model (PSM) into Simple Network Management Protocol SNMP.
SANS Institute [19]. Step by step guide.	Paper discussed command line CISCO IOS configurations. No implementations were recorded.
Auditing and testing CISCO IOS (2003).	Used a Tool called ‘CROCODILE’. Integrated within CISCO router. In the process of auditing and testing, most crucial services were left running.
Fengjiao Li <i>et al.</i> , [11] used a technique called ‘Fuzzing’.	Used ‘fuzzing’ techniques in order to test the CISCO IOS. A script is used to transmit raw packets. CPU usage rocketed to 100%.
Naveed <i>et al.</i> , [22] used SNORT.	Used Access-list controls in order to check authentication settings in IOS router. Software required further fine-tuning.

Another technique used by Naveed *et al.*, [22] used SNORT to create Access List (ACL) rules. ACLs are nothing but a list of allowed and disallowed IP addresses based on network requirements. SNORT was integrated within the routers. ACL rules were detected and configured in case of mal-configuration. SNORT, however, succeeded in preventing intrusion as ACL source packets were blocked. SNORT encountered drawbacks as it turned out to be activity dependent and the system could not be fine-tuned to work well with CISCO IOS. Most studies were in agreement in stressing on the importance of hardening of border routers as they are the first point of entry for any attack or intrusion.

A recent research by Malinowski and Arciuch [23] carried out a thorough study on the implementation of *Dynamic Multipoint Virtual Private Network (DMVPN)*. The main emphasis of the research was based on the importance of DMVPNs, highlighting their functionality of how the protocol is used within a corporate network. A simple topology was created in order to demonstrate his findings. A CISCO router with unknown IOS version was used, however, the router is configured to carry out basic testing. His findings introduced a way of resolving a ‘dead’ IPsec session using cryptographic tunnels created by configuring the router with *Next Hop Redundancy Protocol (NHRP)*.

3. Cryptography and Security

3.1 Overview

Cryptography and its respective keys play a crucial rôle in hardening networks. Intrusion occurs when the penetrators have access to plaintext keys, passwords, data and a blueprint of the network in clear text or in readable form. For a hacker to get access to a network, the first points of entry are the login credentials or crypto-keys. No matter how complex and strict the login passwords are, unencrypted passwords can be easily read and the data can be exploited in order to break into the network, ultimately gaining access to confidential data and information. Data that is

encrypted is known as 'ciphertext'. Data is encrypted from the sender and decrypted at the receiver, using secret keys known as the private and public key. The concept is shown in Fig. 5, below.

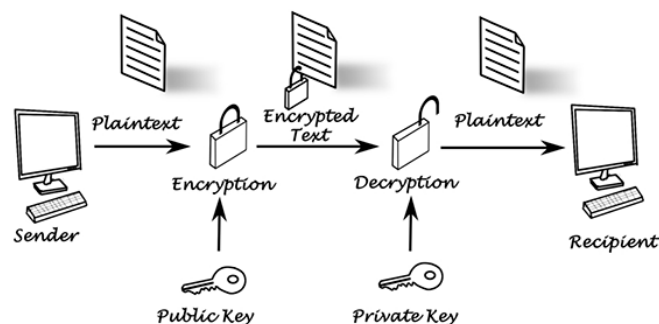


Figure 5. Illustration of Encryption and Decryption [24].

3.2 Cryptography and Security Protocols

Cryptography is widely used in securing networks. It is applicable anywhere in the TCP/IP protocol suite. Strom [25] states that cryptography is also applied to various complicated protocols such as IPsec and DMVPN, they are known as cryptography protocols. In fact, none of the security can be achieved without application of cryptography. Table 2 summarises the routing protocol classification based on security levels.

Table 2. Protocol Classification based on Security Levels.

Protocol	Type	Encryption	Standard	Efficiency	Convergence	Security	Scalable
EIGRP	Interior	Yes	CISCO	Good	Faster	High	Low
OSPF	Interior	Yes	Open	Medium	Faster	High	Low
RIP	Interior	No	YES	Poor	Lower	Low	High

3.2.1 EIGRP (Enhanced Interior Routing Protocol)

Enhanced Interior Gateway Routing Protocol is a CISCO propriety protocol, recommended as best practice for IOS based device configurations. EIGRP exclusively uses Message Digest (MD5) when exchanging encrypted "hello" packets to update its routing table. Unlike, OSPF that keeps records of neighbours, EIGRP keeps a record of the whole topology and has three different type of IP tables that calculates and stores the feasible successor (backup) routes. Furthermore, it also supports summary routes and is ideal for the homogenous environment.

3.2.2 IPsec (Internet Protocol Security) and Virtual Private Network (VPN)

IPsec is widely used for encrypting packets for safe delivery to its destination. CISCO IOS based IPsec-VPN solution allows a remote network to interconnect as a node within the same network. The technology uses tunnels to encrypt the packets and users are able to work as if they are working within the same network [5]. "A remote-access VPN allows a user, with software on her client computer, to connect to a centralized VPN termination device. A site-to-site VPN interconnects two sites without requiring the computers at those sites to have any specialized VPN software installed" [8]. In addition to the appliances such as the ASA firewall and IPSs, IPSEC plays an important rôle in accomplishing network security. IPsec is implemented at the network layer (layer three) of the OSI model. IPsec uses both HMAC-SHA (Hash Message Authentication Code Secure Hash Algorithm) and MD5-SHA (Message Digest 5 – Secure Hash Algorithm) as standard. A typical scenario is shown in Fig. 6, below.

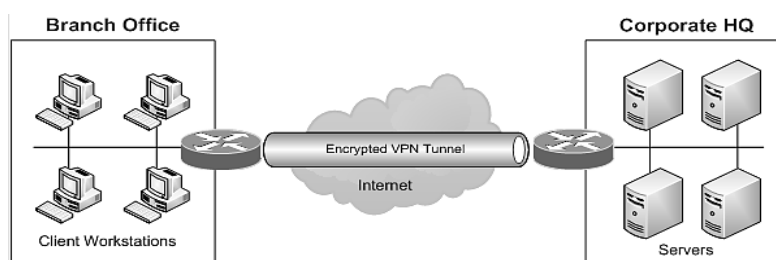


Figure 6. Encrypted Keys and Data Encapsulated within a Tunnel [26].

3.2.3 NHRP (Next Hop Resolution Protocol)

As already explained DMVPNs uses *NHRP*, where one of the routers at the remote site acts as a server (hub) and the rest of the remote site act as a client. The main hub router is configured with its respective *NHRP* IP address. The clients share the same subnet when connecting to sites. When a spoke comes online the hub queries the physical IP address of the router or a client, this helps the hub populate its routing table. The hub stores the physical address registered with each spoke's tunnel IP address.

3.2.4 Generic Route Encapsulation

GRE is probably one of the simpler routing protocols. It encapsulates the traffic within a tunnel. The difference between VPN and GRE is that it is not private. It does not use the VPN IP address but uses its own set of subnets. IPsec can be laid on top of GRE. Unlike IPsec, GRE is capable of routing multicast traffic. GRE is not very effective in an environment where there are too many remote locations, as this will require a full mesh topology. Full mesh topology means that each remote location is directly connected to all other offices and vice-versa. However, DMVPN elucidates the problem.

3.2.5 DMVPN (Dynamic Multipoint Virtual Private Network)

The Hub and Spoke technology is the most commonly used technology within DMVPN where the routers are programmed in such a way that all the traffic from the remote offices will have to pass through the headquarter routers [8]. The protocol provides an economical solution as this eliminates the need for a full-mesh topology. DMVPN is a technology that uses properties of GRE, IPsec and *NHRP* when connecting to a remote office through a Wide Area Network (WAN). DMVPN uses a 'hub' as a central device and all encrypted traffic passes through this router. DMVPN uses *NHRP* that uses a next hop IP address to intelligently route the traffic, in case a router goes down it has a feasible successor i.e. a backup or redundant path. GRE and DMVPN are CISCO proprietary protocols that were implemented in the simulation. Fig. 7, below illustrates data encapsulation within GRE and IPsec tunnel, mGRE is multipoint GRE tunnels.

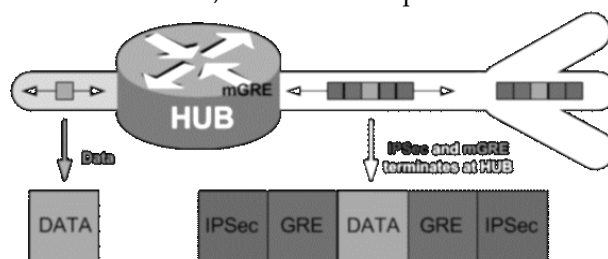


Figure 7. Data encapsulated within GRE and IPsec Tunnel [27].

3.2.6 SSH (Secure Shell)

Secure Shell, or SSH, is a cryptographic (encrypted) network protocol to allow remote login for network administration and management purposes. SSH uses encrypted sessions that use timestamps for security and integrity of transmitted packets. SSH is used as opposed to telnet that

uses clear text passwords and session details. SSH is widely used by network administrators to login remotely into networking devices due its nature of being more secure compared to telnet. It is a good practice to enable SSH on port 22 and disable telnet. Hackers use tools like 'Nmap' to scan open ports in order to initiate any network attack. The SSH port is one of the first things that needs to be exploited. Therefore, SSH implementation with relevant ACL protection is imperative to achieve security at the management level.

3.2.7 IPS (Intrusion Prevention System) within IOS

IPS normally comes as a standalone device that works in a similar fashion to IDS. IPS is capable of not only detecting unwanted traffic but has the ability to block that traffic once it is triggered. Triggering by the IPS is based on both signature files and abnormal behaviour of the network. CISCO Multi-Core routers come equipped with built-in software based IPS integrated within the IOS. The IPS requires public encryption keys and signature files to be uploaded to the flash software by using TFTP (trivial file transfer protocol) as a server. The detection criteria can be set to signature or anomaly based prevention.

4. Defence in Depth

4.1 Overview

The last two decades have been marked by immense growth in the use of the internet. Almost all networks are potentially vulnerable to network intrusions, despite all security measures. In practice, it is never possible to completely secure a system or a network. According to [28], nine out of ten companies have experienced some sort of network attack within the same year. As a result, every year organisations suffer thousands in revenue losses. Security solutions have changed from individual security systems to integrated systems such as routers. However, hardening of these devices is not solely dependent on the available security configurations within the router's operating system. Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack), is an attempt to make a machine or network resource unavailable to its intended users, is the most common attack used by hackers to bring the network down and cause 'one-off' major outage. The 'hacking' side of the security is now shifting to something known as Advanced Persistent Threat (APT), which is another emerging threat to corporate networks.

4.1.1 Components of Defence in Depth

Whilst talking about network security within a corporate or a private network, the importance of perimeters like firewall, IDS, IPS and routers and their configurations cannot be denied. However, appliances like firewall and IDS are standalone devices, before intruders bypass these devices they are routed by layer three devices i.e. routers. The hardening process of CISCO IOS routers is conducted at a later stage of the research project. However, it is important to discuss factors that contribute to securing IOS devices such as the use of cryptographic keys and security protocols that are configured in the routers.

4.2 Advanced Persistent Threat

The most emerging attack that has been a hot topic in the latest research and cyber security conferences is APT. APT are organised cyber-attacks that are on-going. The key difference between conventional hacking and APT is their focus, determination and resources applied to achieve success. In 2010, Google stated that they are in danger of a highly sophisticated and organised attack on their servers, they later named it as APT.

Hackers are mainly an individual or group of people that make use of coding and malicious scripts such as malware, spyware and viruses in order to attack a system. APT, on the other hand, is the long-term surreptitious infiltration of the beleaguered organisation. Howard [29] states that APT sponsors have time, resources and money as political drivers and structured multinationals aid these

groups. In some cases, they are directly funded by the state that changes the game of safety of an organisation. Most of these organised attacks occur at layer three and layer four of the OSI model. This article is mainly focussed towards securing devices at layer three.

4.3 Layers of Defence in Depth

Like any defence system, the concept of defence in depth or Information Assurance (IA) is a multi-layered approach in securing the network or a system. The concept can be closely related to the implementation phase of the project that deals with hardening the router plane-by-plane.

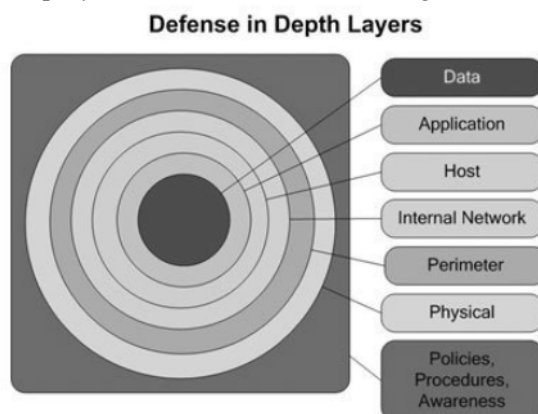


Figure 8. The Concept of Defence in Depth Illustrated as Layers.

Fig. 8, illustrates the layers of defence in depth concept, where the data is secured with multiple layers of security. The data is the main asset of any organisation, therefore, the bulk of the security is applied to secure the Confidentiality, Integrity and Availability (CIA) triad. Implementations of security protocols and encryptions technique is backed up by most secure configurations of management, control and data plane that covers the first five layers of Defence In Depth. The physical security is down to the site management, policies and procedures in place to enforce physical security.

5. Methodology

5.1 Overview

Since the research project is primarily based on a practical implementation, auditing and testing, the outcome of the project relies heavily on the practical implementations and findings thereof. Hence, the research methodology adopted is to implement a network based on real-time emulation software. The software emulates CISCO IOS image and detailed hardening of the 'border router' is carried out based on the implementation of cryptography, encrypted tunnels, crypto-keys and hashing and encryption techniques.

5.2 CISCO IOS versions

One of the latest layer three IOS version 12.4, as shown in Fig. 9, have been emulated at the main border router. Since the nature of the hardening process requires the IOS (router), no switching capabilities are used. However, the switch-ports on layer three devices have been disabled and secured using port security. The following CISCO IOS router images were used:

- Generic GNS3 emulated switches – Access Layer
- CISCO IOS C3750 (Multi-Layered Switch) – Distribution layer
- CISCO IOS C7200 (Layer 3 - HSRP) – Distribution Layer
- CISCO ASA firewall (Layer 4 – 8.42) – For illustration purpose only
- CISCO IOS C7200 (Layer 3 – based on ver. 12.4) – Site 1 Router
- CISCO IOS C7200 (Layer 3 – based on ver. 12.4) – Site 2 Router
- CISCO IOS C7200 (Layer 3 – based on ver. 12.4) – Core '**Border Router**'.

```

Cisco IOS Software, 7200 Software (C7200-JK9S-M), Version 12.4(13b), RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 25-Apr-07 03:18 by prod_rel_team

ROM: ROMMON Emulation Microcode
BOOTLDR: 7200 Software (C7200-JK9S-M), Version 12.4(13b), RELEASE SOFTWARE (fc3)

Border-Router uptime is 2 hours, 24 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"

This product contains cryptographic features and is subject to United

```

Figure 9. Snapshot of the CISCO Internetwork Operating System (IOS) Version.

5.3 Choice of Protocols – Management Plane

The security of the Management Plane was achieved by implementation of the following secured and encrypted protocols:

- Enabling Secure Shell (SSH) and disabling Telnet
- Enabling password encryption service
- Enabling HTTPs server transform
- Enabling SNMPv3 (encrypted protocol) for monitoring purpose.

5.4 Choice of Protocols – Control Plane

Since the project is based on CISCO IOS, Cisco's proprietary EIGRP protocol for routing purposes was used to provide encryption when forwarding traffic. In addition, the Authorisation, Authentication and Accounting (AAA) protocol was configured to fully secure the router's login credential, such as the password in the database. The following encapsulated, encrypted and tunnelling protocols and cryptography techniques were also deployed:

- EIGRP Security
- Message Digest (MD5) – Hashing
- SHA – Hashing
- Advanced Encryption Standards (AES)
- Data Encryption Standard (DES) – 3DES
- Diffie-Hellman Algorithm
- Rivest, Shamir and Adleman (RSA encryption algorithm).

The above encryption methods have been used to generate RSA crypto-keys whilst securing the router's internal planes. These have all been used in conjunction with IKE (Internet Key Exchange) phase 1 and phase 2 when setting up the IPsec VPN (site-to-site).

5.5 Choice of Protocols – Data Plane

The main emphasis is confidentiality and integrity of data. Therefore, multi-layers of security were implemented by making use of IPsec IKE, backed up by application of hashing and encrypted techniques. Also the following cryptographic protocols were deployed:

- Generic Route encapsulation (GRE)
- Multipoint GRE (mGRE)
- Dynamic Multipoint VPN and Next Hop Resolution Protocol (NHRP)
- Hashing and encryption techniques (SHA, MD5, AES, DES etc.)
- Tunnelling Keys (IPsec Phase 1 and 2).

5.6 Software Used

The hardening process requires a number of external software for monitoring, data capturing, analysis of packets/frames and other network services. The following software have been used whilst carrying out the implementation:

- GNS3 – Dynamics
- Solar Winds TFTP server
- Solar Winds SNMPv3 server (Netflow - real-time)
- Wireshark Protocol Analyser
- VM Ware Back Track 5, Ubuntu, Windows 7
- Nmap, CISCO Global Exploit and CISCO Torch
- CISCO Configuration Protocol (CCP) security audit tool.

Fig. 10 shows the framework created for testing hardened CISCO IOS devices based on cryptography and security protocols. Fig. 11, show the Border Area Router where the Cryptography Keys and Protocols are configured.

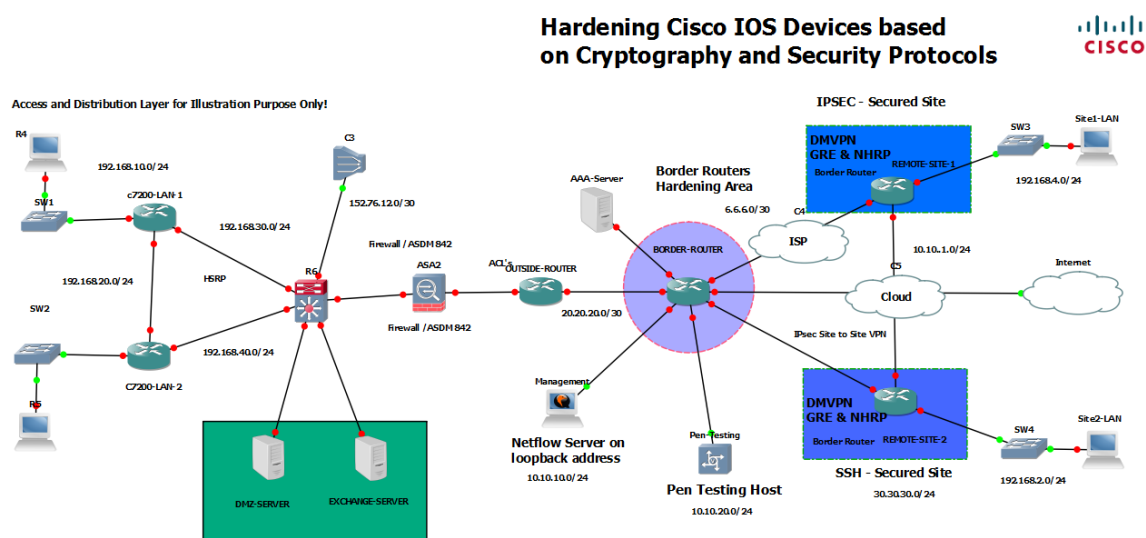


Figure 10. The Framework Created for Testing.

Part 2

The second part of the paper will cover the implementation, testing, critical evaluation, conclusion and further study.

Hardening Cisco IOS Devices based on Cryptography and Security Protocols

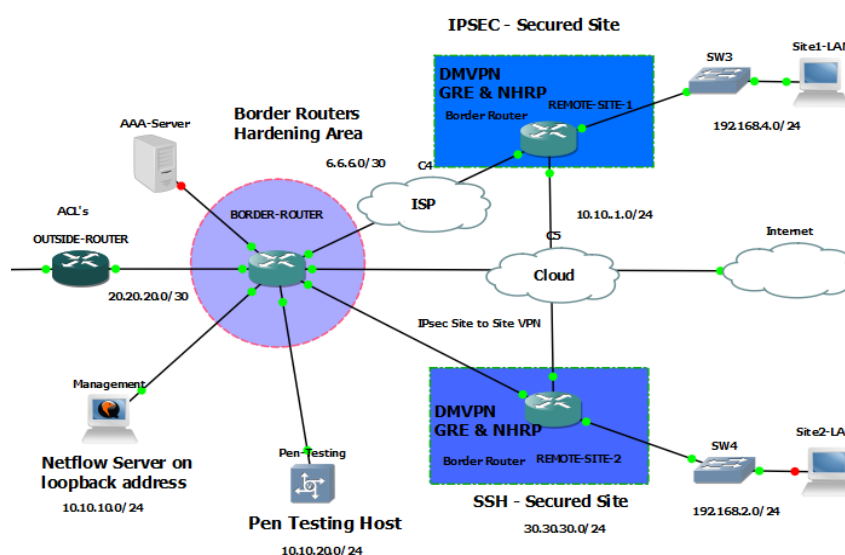


Figure 11. Border Area Router where Cryptography Keys and Protocols are Configured.

References

- [1] Doyle, J., 1998. CCIE Professional Development. Routing TCP/IP, [Online]. 1, 2. Available at: <http://www.CISCOpress.com/series.cfm?series=2&subseries=17&news=0> [Accessed: 30th Nov., 2015].
- [2] Lammle, T., 2013. CCNA Routing and Switching Study Guide. 5th ed. Indiana: John and Wiley Sons, Inc.
- [3] Behrouz A. Forouzan, 2010. TCP/IP Protocol Suite. 4th revised edition. McGraw-Hill Medical Publishing.
- [4] Small Biz trends, (2010), OSI media layer.
Available: <http://smallbiztrends.com/wp-content/uploads/2013/09/osi-model-557x454.gif> [Accessed: 12th Jan., 2016].
- [5] Baker, K., 2014. CCNA Security 640-554 Official Cert Guide. 3rd ed. Indianapolis, USA: CISCO press.
- [6] Symbian, (2013), Data Planes. Available:
http://devlib.symbian.sliions.net/s3/GUID-3D8FE2A7-E544-51B9-9572-492A3B61377C_d0e104753_href.png
[Accessed: 12th Jan., 2016].
- [7] Gregg S., and Smith, D.J., (2008). Router Security Strategies: Securing IP Network Traffic Planes, CISCO Press.
- [8] Wallace, K., 2014. CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. 1st ed. Indianapolis, IN USA: Pearson Education Inc.
- [9] Anrg, (2008), External router. Available: <http://anrg.usc.edu/contiki/images/e/ee/Diagram.png> [Accessed: 3rd Jan., 2016].
- [10] McGee, A.R.; Vasireddy, S.Rao; Xie, Chen; Picklesimer, David D.; Chandrashekhar, Uma; Richman, Steven H., "A framework for ensuring network security", Bell Labs Technical Journal, vol. 8, no. 4, pp.7-27, 2004.
- [11] Fengjiao Li; Luyong Zhang; Dianjun Chen, "Vulnerability mining of CISCO router-based on fuzzing", Systems and Informatics (ICSAI), 2014, 2nd Int. Conf. on, pp. 649-653, 15-17 Nov. 2014.
- [12] Jankuniene, R.; Jankunaite, I., "Route creation influence on DMVPN QoS", Information Technology Interfaces, 2009. ITI '09. Proc. of the ITI 2009 31st Int. Conf. on, pp. 609-614, 22-25 June, 2009.
- [13] Huai Chen, "Design and implementation of secure enterprise network based on DMVPN", Business Management and Electronic Information (BMEI), 2011 Int. Conf. on , vol. 1, pp. 506-511, 13-15 May, 2011.
- [14] Oppenheimer, P, 2011. Top-Down Network Design, 3rd ed. CISCO Press: Indianapolis, IN 46240 USA.
- [15] Tat-Chee Wan; Alwyn Goh; Chin Kiong Ng; Poh, G.S., "Integrating public key cryptography into the simple network management protocol (SNMP) framework", TENCON 2000. Proceedings, vol. 3, pp. 271-276. vol. 3, 2000.
- [16] Hamid R. Nemati, Li Yang (2010). Applied Cryptography for Cyber Security and Defence: Information Encryption and Cyphering, 1st ed., New York: Information Science Reference.
- [17] Yusuf Bhajji, 2008. Network Security Technologies and Solutions (CCIE Prof. Dev. Series). 1st ed. CISCO Press.
- [18] CISCO Press, (2002), Crypto-Tunnel [ONLINE].
Available: https://supportforums.CISCO.com/sites/default/files/legacy/2/7/6/76672-crypto_tunnel.jpg [Accessed: 5th Jan., 2016].
- [19] "The SANS Institute Solaris Step by Step Guide".
Available: <https://itsecurity.gmu.edu/Resources/upload/SolarisSecurity.pdf> [Accessed: 30th June, 2018].
- [20] C. Sheth and R. Thakker, "Performance Evaluation and Comparative Analysis of Network Firewalls", 2011 Int. Conf. on Devices and Communications (ICDeCom), Mesra, 2011, pp. 1-5. DOI: 10.1109/ICDECOM.2011.5738566.
- [21] Peine, H.; Schwarz, R., "A multi-view tool for checking the security semantics of router configurations", Computer Security Applications Conference, 2003. Proceedings. 19th Annual, pp. 56-65, 8-12 Dec., 2003.
- [22] Naveed, M.; UN Nahar, S.; Inayatullah Babar, M., "Network intrusion prevention by configuring ACLs on the routers, based on snort IDS alerts", Emerging Tech. (ICET), 2010, 6th Int. Conf. on, pp. 234-239, 18-19 Oct., 2010.

- [23] Malinowski, T.; Arciuch, A., “The procedure for monitoring and maintaining a network of distributed resources”, Comp. Sci. and Information Systems (FedCSIS), 2014 Federated Conference on, pp.947-954, 7-10 Sept. 2014.
- [24] Make Use Of, (2014), Public Key Encryption.
Available: <http://cdn.makeuseof.com/wp-content/uploads/2015/02/public-key-encryption.png?6b9ecc> [Accessed: 16th March, 2016].
- [25] Strom, S, 2003. The importance of Cryptography in Network Security. 2D1441 Sem. in Theoret. Comp. Sci., 01, 5.
- [26] Information Security Institute, (2015), Encrypted VPN Tunnel.
Available: <http://cdn.makeuseof.com/wp-content/uploads/2015/02/public-key-encryption.png?6b9ecc> [Accessed: 24th March, 2016].
- [27] Firewall CX, (2015), DMVPN IPsec in tunnel mode.
Available: <http://www.firewall.cx/images/stories/CISCO-dmvpn-single-dual-tier-2.png> [Accessed: 30th March, 2016].
- [28] Hackmagadoon, (2015), Cyber-attacks.
Available: <https://paulsparrows.files.wordpress.com/2015/05/motivations-apr-2015.png> [Accessed: 13th Dec., 2015].
- [29] Howard D. (2011) Security 2020: Reduce Security Risks This Decade, Indianapolis, IN: Wiley Publishing.



© 2018 by the author(s). Published by Annals of Emerging Technologies in Computing (AETiC), under the terms and conditions of the Creative Commons Attribution (CC BY) license which can be accessed at <http://creativecommons.org/licenses/by/4.0/>