Comprehensive Network Security Approach: Security Breaches at Retail company- A Case Study

Mehdi Jahanirad, Yahya AL-Nabhani, Rafidah Md.Noor

Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

Abstract

The development of the Web technologies and services increases the level of threats to data security in companies and enterprises day by day. As criminals are turn into professional network intruders, new laws and legislations are introduced to cover information security. Even though on-line businesses provide the productivity and efficiency advantages, without the comprehensive network security plan an online retail company which operates with information systems about its daily businesses, increases its risk to become vulnerable to security breaches. The purpose of this article is to introduce a comprehensive network security approach for an online retail company which suffers from security breaches. This article begins with the brief introduction about the problem statement and the proposed method to complete the security enhancement. Next, an ideal network architecture suggested, using both basic network diagram and security enhancement network diagram. The recent task will be continued by implementing the security and password policies to the network. Finally the whole procedure will be simulated and examined using Cisco Packet Tracer Experiment. The simulation results show that the approach was successful in designing a comprehensive network security, and to defend the company against security breaches.

1. Introduction

The deployment of the technology with retail companies brought many advantages to business industries such as cutting costs, increasing revenue opportunities and being more responsive to their customers' needs. In other perspective the only way to achieve these advantages is to secure the fundamental technologies, which may suffer from vulnerabilities that can be exploited by expert attackers. The objective of these attackers is not anymore limited to demonstrating their ability to compromise a system, but they are members of profit-obsessed illegal institutes whom aim to attain login permits to financial sites for financial thievery, identity thievery and pump-and-dump stock systems. Considering the rapid growth of the malevolent attacks, business and government rule makers demand constantly strong security to let IT meet contentment otherwise encounter formal sentences (SonicWALL, 2008).

Security breaches are generally classified as illegal data surveillance, faulty data re-editing, and data engagement. Illegal data surveillance cause the expose of information to users not permitted to obtain access to this information. All companies, varying from profitable companies to public companies, in different fields such as healthcare and homeland protection, may experience serious losses from both financial and individual perspective as a result of illegal data surveillance. Faulty data re-editing, whither it is on purpose or not it will cause faulty database situation. In case data is engaged, the vital information for the right performance of the company is not promptly accessible when required (Bertino & Sandhu, 2005).

Watkins & Wallace (2008) argued that the main reason for occurrence of security breaches within an organization is the lack of security policy or, if a security policy is in place, the lack of effectively communicating that security policy to all concerned. Policy sets in Network are sets of the Network object that pass through or into a router. The three types of network object that the routers process are IP addresses, packets and routes (Sedayao, 2001).

This article discusses the outcome of the implementation of the security enhancement for the retail company's security case using the Packet Tracer Experiment. This scenario is the case referred to the team of consultant by the online retail company subsequent to a security breach, only after 8 hour they could return the system to its normal condition. The team realize that this situation didn't happen for the first time in this company and they had previously experienced two 1 hour disruption this year before the existing attack. The company is an online retail unit which should be available to its customers 24 hours for every day and 7 days for every week. The proposed solution by the team of consultant includes two assignments. The article discusses the first assignment in section 2, to suggest the network architecture using the basic network diagram and security enhancement diagram, in section 3 implements the security and password policy into the network diagram, in section 4 the complete network security strategy will be simulated and tested using Packet Tracer Experiment, in section 4 the results and security performance will be concluded.

Manuscript received August 5, 2012
Manuscript revised August 20, 2012

2. Network Architecture

One of the most critical and complicated challenges regarding to network design is to build security approaches which are able to secure all components of the perplex network without interfering with on its usability and functionality (Oppenheimer, 2011). In order to accomplish commercial and industrial objectives of a company, the recommended network topology shall have numerous interconnected components. The most supreme method is to build the hierarchical, multi layered network design pattern which build in distinct layers. Every layer has to concentrate on precise tasks permitting the selection of the right methods and attributes for the layer.

Oppenheimer (2011) in his book discussed a hierarchical topology in three layers, a core layer, distribution layer and access layer,

- A core layer consists of high-end routers and switches which are optimized for ease of use and speed
- A distribution layer consist of routers and switches which apply policies and partition traffic
- An access layer link up users using hubs, switches, and other devices

In the same book he has summarized the most important factors in network design as below:

- Using an organized, top-down methodology
- Arranging the logical design ahead of the physical design
- The design of the topology should have hierarchy, redundancy, modularity, and security

SAFE is a reference architecture which might be used by network engineers to make easier the convolution of a bulky internetwork. Cisco SAFE architecture is especially concerned with security. SAFE takes a defense-indepth approach, while several layers of protection are strategically located all over the network. The layers are under a unified strategy for protecting the entire network and the various components of the network, including individual network segments, infrastructure devices, network services, endpoints, and applications (Oppenheimer, 2011). Figure 2-1 shows the main modules in the SAFE security reference architecture.

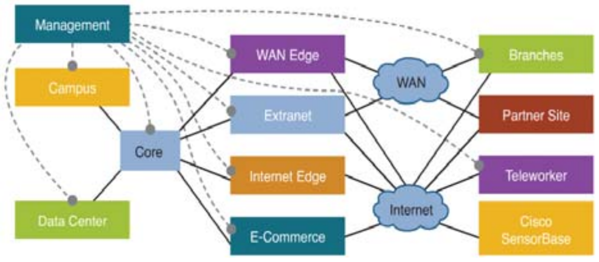


Figure 1. High-Level View of Cisco SAFE Architecture (Oppenheimer, 2011)

SAFE architecture as shown in Figure 2-1 comprises elements in three layers, the first layer or Site Edge contains modules such as management, campus and data center to build a robust site network that provide high availability, scalability, and flexibility. The second layer or Company Edge restrain all the network components for professional and safe transmission between the company site and isolated spots, these modules are WAN edge, Extranet, Internet edge and E-Commerce. The third layer or service provider edge contains modules such as Branches, Partner Site, Teleworker and Cisco SensorBase. The core modules provide reliable and scalable Layer 2 and Layer 3 transport. Layer 2 is interconnected with Layer 3 through internet and WAN.

2.1 Basic Network Diagram

The given case studied by this article describes the company's network architecture as below. "The network administrator works at Site A, one of many sites within a large, geographically dispersed Intranet. The company has two connections to the Internet through different Internet Service providers (ISPs), both at the same bandwidth. This has been implemented to provide backup routing in case one connection goes down. Because a routing policy has not been implemented to enforce this preference, all Internet IP traffic passes through the usage-based connection, forcing the company to incur higher than necessary costs." Table 2-1 consists of the devices which will generate the network architecture.

Figure 2-1shows the basic network architecture which has been created using the specifications written in Table 2-1 in Cisco Packet Tracer. Now that the main architecture has build, the proposed security enhancement generates an ideal network.

Table 2-1Network's components Table

	Site A	Site B	Site C
IP Address	192.168.30.0/24	192.168.65.0/24	192.168.28.0/24
Router	A&B	BR-1	BR-2
Server	Web Server	Web Server	Web Server
Host	8 Host divided into 2 Subnets using Switches.	8 Host divided into 2 Subnets using Switches.	8 Host divided into 2 Subnets using Switches.

The basic network diagram shows the Cisco network topology, Site A (192.168.30.0/24) contains two routers, Router A and Router B. Site B (192.168.65.0/24) is connected to Site A via border router 1(BR-1) and connects to Site C (192.168.28.0/24) via border router 2(BR-2). Two different connections to the internet provided using the two ISPs both at the same bandwidth.

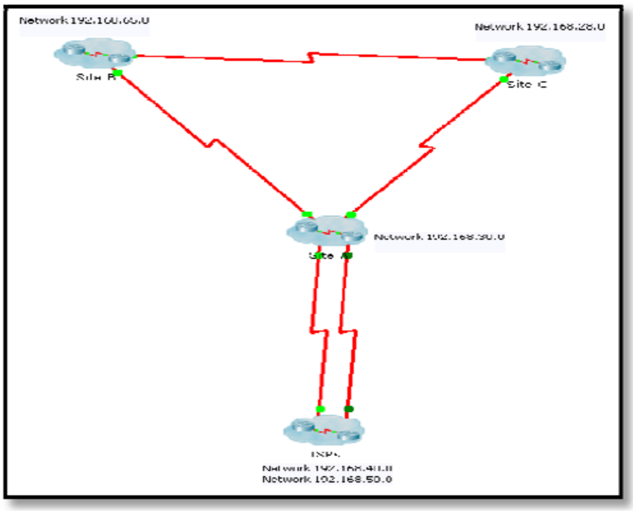


Figure 2. Basic Network Diagram

2.2 Security Enhancement Network Diagram

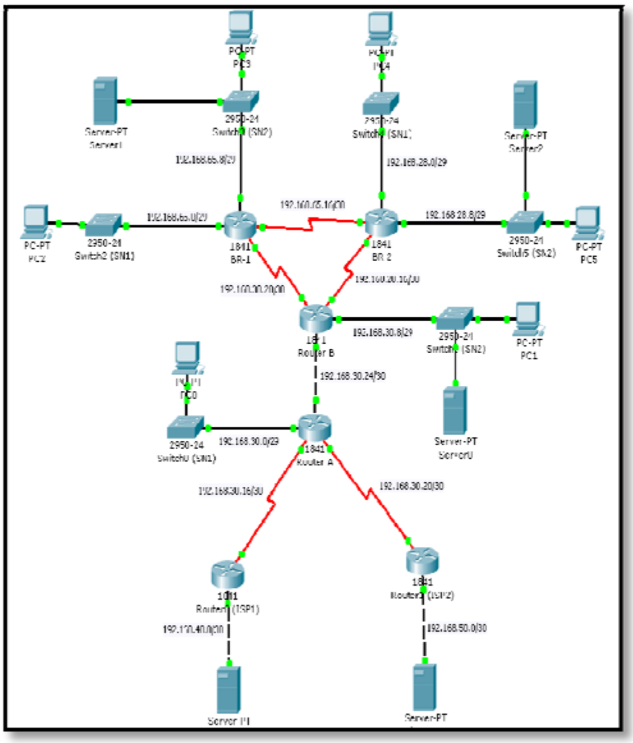


Figure 3. Security Enhancement Network Diagram

Figure 2-3 illustrates the security enhancement network diagram, to prove the security function of this topology; it can be compared with the Cisco SAFE security reference architecture discussed in the beginning of this section. ISP1 and ISP2 are two correspondence routers both connected to the Web Server demonstrate the service provider edge or third layer. Site A with two routers A and B provides service to 8 hosts which are divided into 2 subnets and retain Web server connection. This Site exhibits second layer or enterprise edge which provides isolation point between first and third layer of the network. This layer should embrace overprotective admission to sources for security purposes, and overprotective network traffic which goes over the core for accomplishment purposes. The members of Site B and C, hosts and switches are the modules of the first layer or campus edge and BR-1 and BR-2 represent core module in Cisco SAFE security reference architecture, which provide consistent and measurable Layer 2 and Layer 3communication. It is advisable for the company to hold any data that should not be accessible by the general public in first layer or campus edge.

3. Security & Password Policy

Most of the attacks on an organization‘s computer resources originate from the inside network, while the internal threats tends to be more serious than external threats. The reason is the inside users have more knowledge of the network and its available resources, they have more level of access granted to them due to their job responsibility and also custom network security mechanism such as Intrusion Prevention System (IPS) and firewalls are of no use next to these types of threats. A security and password policy is one of the most effective key solutions to this category of threats.

A security policy is a continually changing document that dictates a set of guidelines for network use. These guidelines complement organizational objectives by specifying rules for how a network is used. The main purpose of a security policy is to protect an organization's assets. An organization's assets include more than just tangible items. Assets also entail such things as intellectual property, processes and procedures, sensitive customer data, and specific server functions (for example, e-mail or web functions) (Watkins & Wallace, 2008). Watkins & Wallace (2008) argued in this book that other than protecting organizational assets, a security policy serves other purposes, such as the following:

- Making employees aware of their obligations as far as security practices
- Identifying specific security solutions required to meet the goals of the security policy
- Acting as a baseline for ongoing security monitoring

One of the first steps in security design is developing a security plan. A security plan should reference the network topology and include a list of network services that will be provided (for example, FTP, web, email, and so on). This list should specify who provides the services, who has access to the services, how access is provided, and who administers the services.

The components of security policy are, access policy, accountability policy, authentication policy, privacy policy and computer-technology purchasing guidelines. The security policies will be implemented using security procedures. Procedures define configuration, login, audit, and maintenance processes.

3.1 Policy Sets in Network

In network policies, policy sets are sets of the network objects that pass through or into a router. The three types of network objects that routers processes are host IP addresses, packets, and routes. Network administrators implement policies by defining policy sets of these objects and applying rules to them. The policies are enforced as routers check the host IP addresses, packets, and network numbers going through them to see if they are members of a defined policy set. If so, rules are applied to those network objects. To accomplish this assignment the following policies are implemented in the company's network diagram:

a. Policy Set #1: All routes going through Site A. This type of policy deals with scenarios where for business reasons like cost, certain network paths are preferred.

In this case network traffic has to pass just through Site A being a final route. As a result, traffic should not go through Site A unless no other route is available. Traffic won't stream through a router to a given destination unless routing information exists for that destination, this policy can be implemented by defining a policy set of all the routes going through Site A. On the other hand, since in this situation there is no other route, in order to connect the ISPs. Thus, there is no need to block any type of traffic.

b. Policy Set #2: Host with IP addresses in network 192.168.30.0/24. Only host in this network set to log into Router A and Router B.

The following policy set implemented using the Standard Cisco Access Control List (ACL). A Standard Access List only allows the organization to permit or deny traffic from specific IP addresses. Standard IP Access List applied in Site A router A in order to allow the hosts in this subnet to access router A and B. The entries are in following order:

```
   Router  A(config)#access-list  1  permit
192.168.30.0 0.0.0.7
   // the policy applied in interface
   Router A(config)#interface f0/1
```

The same steps are repeated in router B in order to allow the hosts in subnet B to access router A and B. The entries are in following order:

```
Router A(config-if)#ip access-group 1 in
```

```
   Router  B(config)#access-list  2  permit
192.168.30.8 0.0.0.7
   //the policy applied in interface
   Router B(config)#interface f0/1
   Router B(config-if)#ip access-group 1 in
```

c. Policy Set #3: HTTP Packet to Hosts in Subnet 1 in each site (Site A, Site B and Site C). Only web traffic is allowed in Subnet 1.
This policy set has to be formed using another type of network object which is packet. To allow a packet only in specific locations in the network it is an Extended ACL that has to be used. The entries created for every respective site are as following:

(1) Site A

```
Policy Set #101: HTTP packets to the
host at Subnet 1 in Site A
Policy Set #101: No other packets
Router A(config)#access-list 101 permit tcp
0.0.0.0     255.255.255.255     192.168.30.0
0.0.0.7 eq 80
Router  A(config)#access-list  101  deny  ip
0.0.0.0     255.255.255.255     192.168.30.0
0.0.0.7
Ethernet interface 0/1: Apply Policy
Set #101 to outgoing packets in router
A
Router A(config)#interface f0/1
Router A(config-if)#ip access-group 101 out
```

(2) Site B

```
Policy Set #102: HTTP packets to the
host at Subnet 1 in Site B (BR-1
Router)
Policy Set #102: No other packets
BR-1(config)#access-list  102  permit  tcp
0.0.0.0     255.255.255.255     192.168.65.0
0.0.0.7 eq 80
BR-1(config)#access-list   102   deny   ip
0.0.0.0     255.255.255.255     192.168.65.0
0.0.0.7
Ethernet interface 0/0: Apply Policy
Set #102 to outgoing packets in router
BR-1
BR-1(config)#interface f0/0
BR-1(config-if)#ip access-group 102 out
```

(3) Site C

```
Policy Set #103: HTTP packets to the
host at Subnet 1 in Site C
Policy Set #103: No other packets
BR-2(config)#access-list 103 permit tcp
0.0.0.0  255.255.255.255  192.168.28.0
0.0.0.7 eq 80
BR-2(config)#access-list 103 deny ip
0.0.0.0  255.255.255.255  192.168.28.0
0.0.0.7
Ethernet interface 0/0: Apply Policy
Set #103 to outgoing packets in router
BR-2
BR-2(config)#interface f0/0
BR-2(config-if)#ip access-group 103 out
```

d. Policy Set #4: SSL packets to the host at Web Server.

(1) Site A (Router B)

```
Policy Set #104: SSL packets to the
host at Subnet B in Site A (Router B)
Policy Set #104: No other packets
Router B(config)#access-list 104 permit tcp
0.0.0.0    255.255.255.255    192.168.30.8
0.0.0.7 eq 443
Router B(config)#access-list 104 deny ip
0.0.0.0    255.255.255.255    192.168.30.8
0.0.0.7
Ethernet interface 0/1: Apply Policy
Set #104 to outgoing packets in router
B
Router B(config)#interface f0/1
Router B(config-if)#ip access-group 104 out
ip access-group 104 out
```

(2) Site B (BR-1 Router)

```
Policy Set #105: SSL packets to the
host at Subnet B in Site B (Router BR-
1)
Policy Set #105: No other packets
BR-1(config)#access-list 105 permit tcp
0.0.0.0    255.255.255.255    192.168.65.8
0.0.0.7 eq 443
BR-1(config)#access-list 105 deny ip
0.0.0.0    255.255.255.255    192.168.65.8
0.0.0.7
Ethernet interface 0/1: Apply Policy
Set #105 to outgoing packets in router
BR-1
BR-1(config)#interface f0/1
BR-1(config-if)#ip access-group 105 out
```

e. Policy Set #5: Border Router 2 (BR-2) has two interfaces, Ethernet 0 and Ethernet 1. Network 192.168.28.0/24, where the payroll hosts live in (Subnet 2), is on the Ethernet 1 interface. They wish to limit access to the payroll systems on the Subnet 2 network to the following hosts in Subnet 1 (Site C). The hosts in Subnet 1 can send any kind of IP traffic to the other Subnets in Site A and B. No other hosts have any business with the payroll systems and should have no access whatsoever.

Site C (BR-2 Router)

Policy set #5a: No other hosts have any business with the payroll systems and should have no access whatsoever.

In order to prevent any access to subnet 2 (payroll subnet) in site C the following police are set in BR-2;

```
BR-2(config)#access-list    5    permit
192.168.28.0 0.0.0.8
BR-2(config)#access-list 5 deny any
```

The policy should be applied in payroll subnet interface as following,

```
BR-2(config)#interface f0/1
BR-2(config)#ip access-group 5 out
```

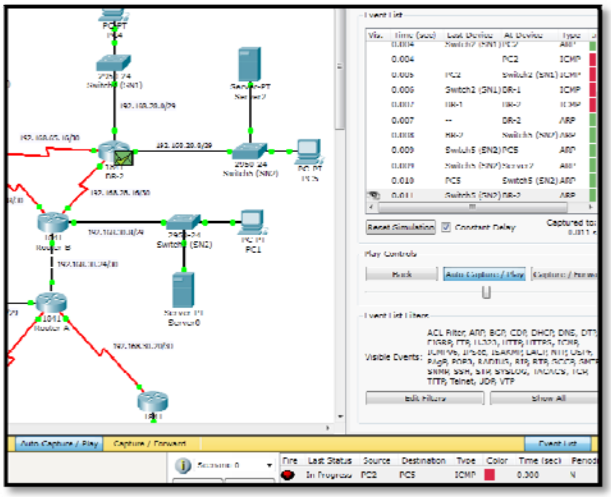
Policy set #5b: The hosts in Subnet 1 can send any kind of IP traffic to the other Subnets in Site A and B.

```
BR-2(config)#access-list 106 permit
ip 192.168.28.0 0.0.0.7
192.168.30.0  0.0.0.7
BR-2(config)#access-list 106 permit
ip 192.168.28.0 0.0.0.7
192.168.30.8  0.0.0.7
BR-2(config)#access-list 106 permit
ip 192.168.28.0 0.0.0.7
192.168.65.0  0.0.0.7
BR-2(config)#access-list 106 permit
ip 192.168.28.0 0.0.0.7
192.168.65.8  0.0.0.7
Router(config)# int f0/0
Router(config-if)# ip access-
group 106 in
```

4. Packet Tracer Experiment

Packet Tracer is a protocol simulator build by Dennis Frezzo and his coworkers in Cisco Systems. Packet Tracer is a strong, dynamic and open source tool which provides simulation, visualization, authoring, assessment and collaboration capabilities and facilitates the teaching and learning of complex technology concepts (Cisco Systems, 2010).

The studied topology build in Packet Tracer, and the policy has been set. In the bottom of the window inside the task bar the status of the connection is written, the network architecture is proved to work in full performance in both before and after application of the network policy, because every network component follow the approached solution for the company's network design.



Event List

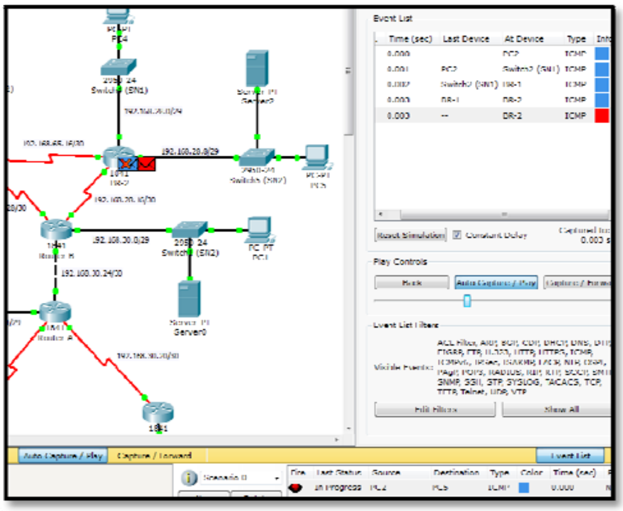
Vis.	Time (sec)	Last Device	At Device	Type
	0.004	Switch2 (SN1)	PC2	ARP
	0.004		PC2	ICMP
	0.005	PC2	Switch2 (SN1)	ICMP
	0.006	Switch2 (SN1)	BR-1	ICMP
	0.007	BR-1	BR-2	ICMP
	0.007	--	BR-2	ARP
	0.008	BR-2	Switch5 (SN2)	ARP
	0.009	Switch5 (SN2)	PC5	ARP
	0.009	Switch5 (SN2)	Server2	ARP
	0.010	PC5	Switch5 (SN2)	ARP
	0.011	Switch5 (SN2)	BR-2	ARP

Reset Simulation ☑ Constant Delay Captured to: 0.011 s

Visible Events: ACL Filter, ARP, BGP, CDP, DHCP, DNS, DTP, EIGRP, FTP, H.323, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NTP, OSPF, PAgP, POP3, RADIUS, RIP, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Period
●	In Progress	PC2	PC5	ICMP	🟥	0.000	N

Figure 4. Pcket transfer simulation before applying the poicy set



Event List

	Time (sec)	Last Device	At Device	Type	Info
	0.000		PC2	ICMP	🟦
	0.001	PC2	Switch2 (SN1)	ICMP	🟦
	0.002	Switch2 (SN1)	BR-1	ICMP	🟦
	0.003	BR-1	BR-2	ICMP	🟦
	0.003	--	BR-2	ICMP	🟥

Reset Simulation ☑ Constant Delay Captured to: 0.003 s

Visible Events: ACL Filter, ARP, BGP, CDP, DHCP, DNS, DTP, EIGRP, FTP, H.323, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NTP, OSPF, PAgP, POP3, RADIUS, RIP, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Fire	Last Status	Source	Destination	Type	Color	Time (sec)
●	In Progress	PC2	PC5	ICMP	🟦	0.000

Figure 5. Packet transfer simulation after applying the policy set

Figure 4.1 illustrates the result of the simulation of the network before applying the security, the packet transfers between the two network components, PC2 in Site B and PC5 in Site C, which are selected using an action named Ping. The simulation shows the packet transferred from PC2 and passed from router BR-1, and then it proceeded successfully to the BR-2 router in Site C and received to PC5.

Figure 4.2 shows the result of the simulation of the network after applying all the policy sets, this illustration is the simulation of the packet transfer between the same network components as used in illustration in Figure 4.1, the reason to perform the experiment for Site C is that this Site is the module of first layer, and most of the policies are applied to this layer .The simulation shows the packet transferred from PC2 in Site A to BR-1 router, and then it passed to BR-2 router in Site C, but due to policies set in BR-2 router the packet transfer is unsuccessful from this router.

5. Conclusion

To suggest the comprehensive security approach to the studied retail company many theoretical features discussed in the literature. The previous studies on the design of the network architecture helped to design the attractive topology, the security features are also considered in the arrangement of the topology. Secondly the use of Security and Password policy to provide security in the architecture studied and implemented in 5 different policy sets that pass into routers. In the end both network topologies, the one without security policy and the one with it are simulated using Cisco Packet Tracer Experiment. The simulation results prove that both architectures are work properly and the configuration results show the correct interconnection of the network components.

In summary this paper provided the solution to the security breaches in the studied retail company, by providing the enhancement in network topology from the security perspective and assigning policy to its routers.

References

[1] Bertino, E., & Sanhu, R. (2005). Database Security-Concept, Approaches, and Challenges. IEEE Transactions on Dependable and Secure Computing, Volume 2, No.1.

[2] Cisco Systems (2010). Cisco Packet Tracer : At a Glance. Available at http://www.cisco.com/web/learning/netacad/course_catalog/docs/Cisco_PacketTracer_AAG.pdf

[3] Oppenheimer, P. (2010). Top-Down Network Design. Indianapolice: CiscoPress. 3rd ed.

[4] Sedayao, J. (2001). Cisco IOS Access Lists. O'Reilly.

[5] SonicWALL (2008). Retail: Securing the Competitive Edge with Technology. Available at http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=WP&id=56

[6] Watkins, M., & Wallace, K. CCNA Security: Official Exam Certification Guid. Indianapolice: CiscoPress.