Global Information Assurance Certification Paper

Research on: Hardware Encryptor and Internet Firewall

Author: Bin Zhong
Date: June 27, 2003
Assignment: V1.4b Option #1

Table of Contents

Abstract

More and more people will prefer to separate VPN and Firewall, so they can shift the load off the firewall, also it will simplify the configuration, maintenance and troubleshooting.
At the same time, some big companies also provide some hardware Encryptor solution, such as Thales Datacryptor™ 2000[1] [2], Nokia Crypto Cluster[3] and Cisco VPN Concentrator[4] [5]. It becomes popular to have dedicated hardware Encryptor and firewall to work together at company gateway.

For some big companies, their internet gateway system are already quite complex, after putting the hardware Encryptor box in, it will create a lot of issues, such as location of Encryptor, security issue, routing issue, load issue and NAT issues etc. This paper is a research on the issues we are facing, how to choose the solution. Below we will discuss three options: Hardware Encryptor without Firewall, Hardware Encryptor with Single Layer Firewall and Hardware Encryptor with Double Layer Firewall.

Hardware Encryptor without Firewall

Now some companies do not trust the dedicated link provided by Telecom Companies, they want to encrypt the traffic between branches. Also for cost-saving or second backup line, they will use local ISP to connect Internet locally, and then VPN all branches together (See figure1).

---

[1] Racal Security and Payments. "Network Security and VPN solutions" URL: http://www.parallaxresearch.com/dataclips/pub/infotech/protocols/VPN/Security_and_VPNs.PDF

2 Thales-esecurity.com "Embedded Router Encryption-AN Analysis of Security Weaknesses". URL http://www.thales-esecurity.com/CMS/docs/encryption.pdf

3 Nokia Ltd " Nokia VPN Gateway Administrator", Version 1.0 Sep 2000, Pages 15-32

4 Cisco.com "Cisco VPN 3000 Concentrator and Client Frequently Asked Questions" Apr 15, 2003. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_qanda_item09186a0080094cf4.shtml#Q3

5 Cisco.com "Understanding the VPN 3000 Concentrator" URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_chapter09186a00800bf699.html#xtocid4

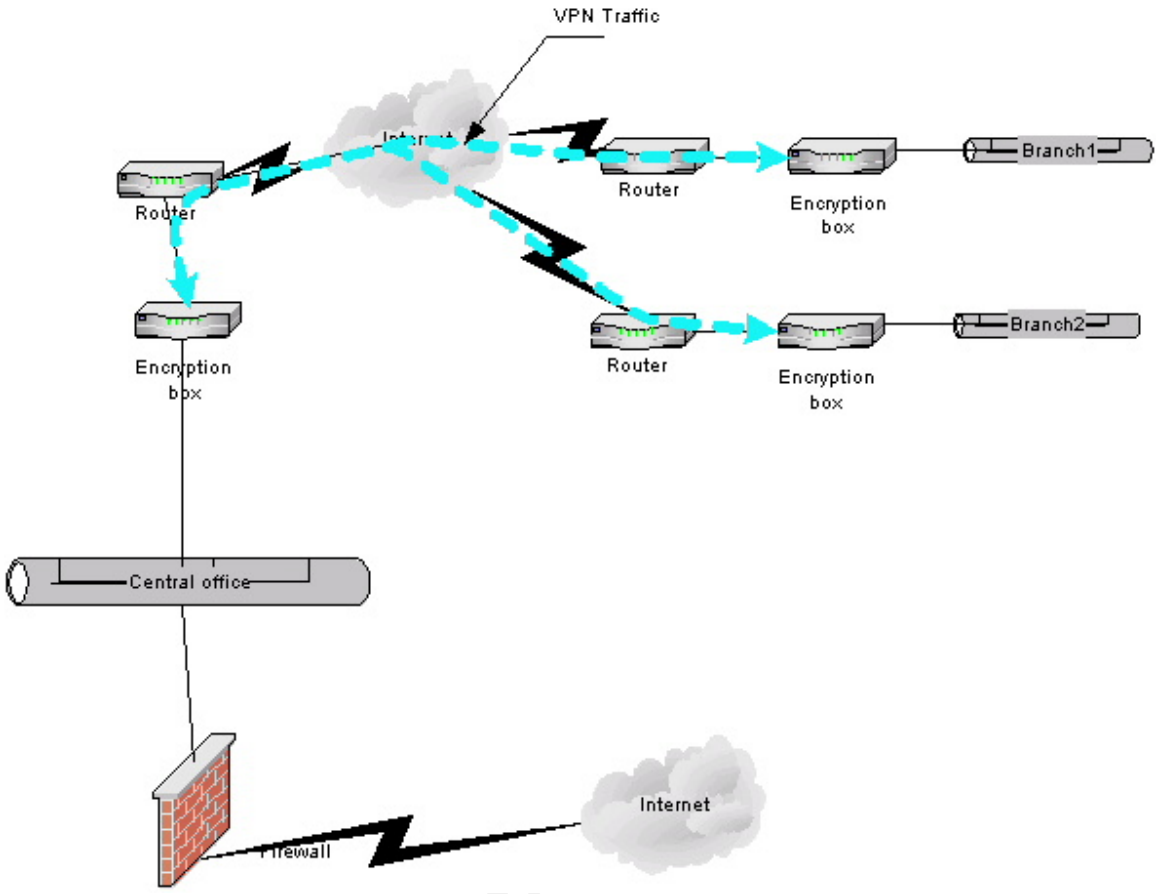

Figure1

Using hardware Encryptor box will be very good solution, it need a little maintenance, for most of case, you don't need upgrade patches as often as firewall, normally cheaper than firewall /VPN solution.

But for HTTP browsing traffic and email traffic from the branch offices, you need transfer the traffic twice on the internet, one form branch to central office, another one form central office to Internet, then you need pay almost double for the kind of the Internet traffic. For most of hardware Encryptors, they have some IP filter functions build in, you can use that to basic firewall to allow HTTP, SMTP traffic to pass out locally through local ISP. However, this kind of filter normally is not strong as firewall, and don't have central management tool for local filter in VPN box, so you need configure each box individually. Sometime, it will end up with big hole in some branches, and then through that, hacker can break into whole company network.

It is recommended to using VPN box as pure VPN box, and then locked down all ports except IPSEC port and management port. Using gateway system of central office as only gateway to Internet, to provide more central management and security.

At this solution, encrypted and unencrypted traffic don't need pass through firewall. Central office and remote branches are virtual local LAN through VPN, which is encrypted by hardware VPN boxes. But as we have talked before, the branches internet browsing and email traffic will transfer twice, and you need pay double for the kind of traffic from the branch offices, also if central office Internet link is down, all branches will lost Internet connection. If for company, central office is very big, the branch offices are quite small, maybe just a few of employers, it is quite good. But for some company, each site have almost same amount of employers, passing all traffic to one central point, then pass traffic from central point to internet, is not so efficient and economical. They need install firewall working with VPN box.

Hardware Encryptor With Single Layer Firewall

In Front Of Firewall

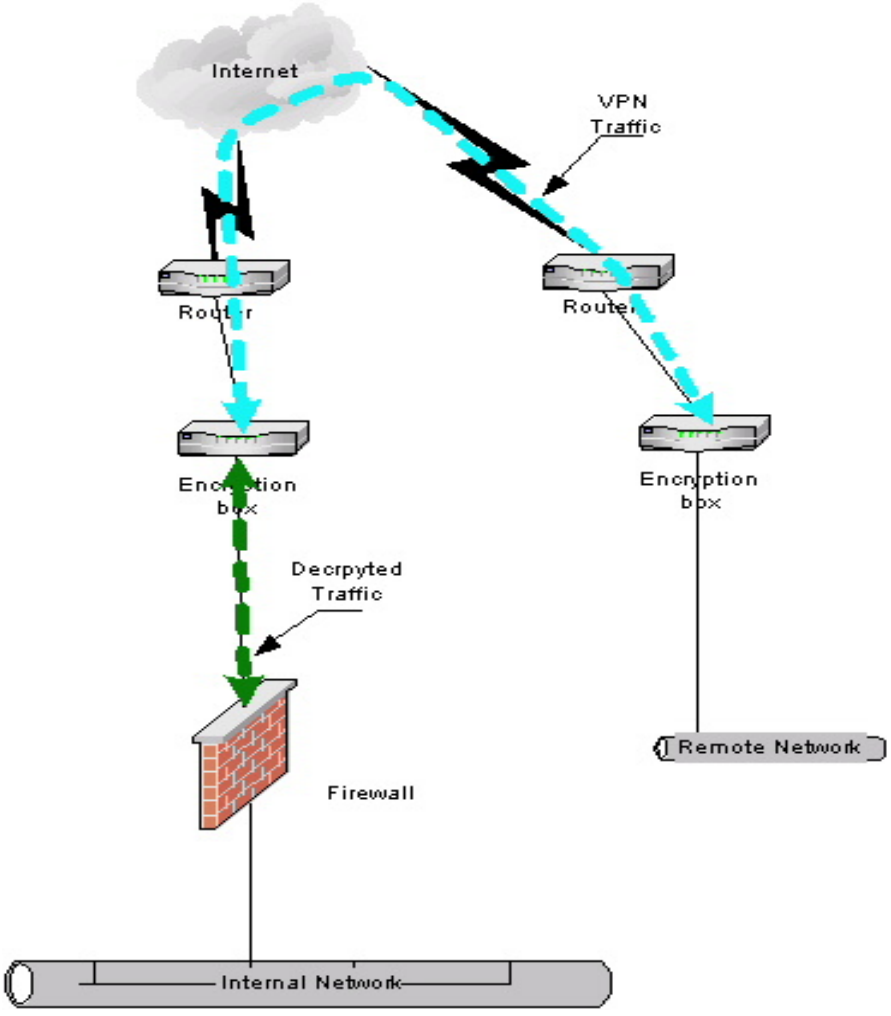

Figure2

For the case (see Figure2), traffic is decrypted before it hits the firewall, you can apply firewall policy to packets since firewall can see all VPN traffic, and firewall don't have to know about VPN protocols.

But that also mean firewall can't tell whether the packets were encrypted before it hit the firewall. The encryption box is not protected by firewall.

The traffic between VPN box and firewall is not encrypted; you will exposure your internal traffic to Internet. So using cross over cable to connect two box together will prevent someone to add one more box by accident, then hacker can see all internal traffic by hijacking the box.

For non-IP traffic, such as IPX, NetBEUI etc, you can't use the solution, because most of Internet firewalls don't support the kind of non-IP traffic.

In the situation, encryption box will decide which traffic will be decrypted, which traffic just pass to firewall, or drop. So encryption box must have filter function, otherwise, the solution doesn't work.

Routing is quite simple. For outgoing traffic, firewall have default gateway to encryption box, encryption box have default gateway to external router, if traffic is going to remote network or remote client, then encrypt it, otherwise, pass it in clear. For incoming traffic, external router forwards all incoming traffic to encryption box, then encryption box will decide to decrypt traffic, or pass it, then forwards all traffic to firewall to filter traffic.

Because firewall must have legal IP address, in this configuration, you will need one more subnet legal IP addresses.

Fortunately, for legal IP address problem and easy implementation, we can stick the VPN box outside of firewall or called "one-armed VPN in front of firewall", (see Figure 3)

For the solution, you don't need change whole gateway architecture, all you need is one external IP address, then you can install VPN box, but internal interface of external router will see both encrypted and unencrypted traffic, and you can't use crossover cable to connect VPN box and external router, so using switch is better than using hub, because switch will separate traffic. Also you should don't allow people to put more box into this switch.

Also routing will be a little bit complex. For the case, you have two routing options.

Option1, same as VPN box in front of firewall.
For outgoing traffic, firewall forwards all traffic to VPN box, then VPN box decide which traffic is encrypted, then forwards all traffic to external router.

For incoming traffic, external router forwards all traffic to VPN box, then VPN box decide which traffic will be decrypted, then forwards all traffic to firewall.
For this case, because all incoming and outgoing traffic both go through same network interface of VPN box, each packet will transfer twice in same network interface, so if the VPN box have 10M-network interface, then maximum throughput will be 5M.

Option 2, if your external router, load-balance product, and firewall are intelligent enough to route traffic by protocol, then you can use the option 2.

For outgoing traffic, firewall will decide if the traffic needs to be encrypted, then pass it VPN box, otherwise pass it to external router directly. For fixed IP address of remote VPN box, you can route outgoing traffic by remote IP address. But for no-fixed IP address at remote end, you don't know how to route traffic, so you must use option 1.

For incoming traffic, external router or load–balance product will decide, if the traffic need to be decrypted, then pass it to VPN box, otherwise, pass it to firewall directly. How to decide which traffic should be encrypted or decrypted, will base on how to implement VPN, if remote site have fixed IP address, you can route by IP address, if remote site don't have fixed IP address, then you just can route traffic by encryption protocol.

For option 2, less traffic passes to VPN box than Option1, so performance of VPN box will be better than Option1.

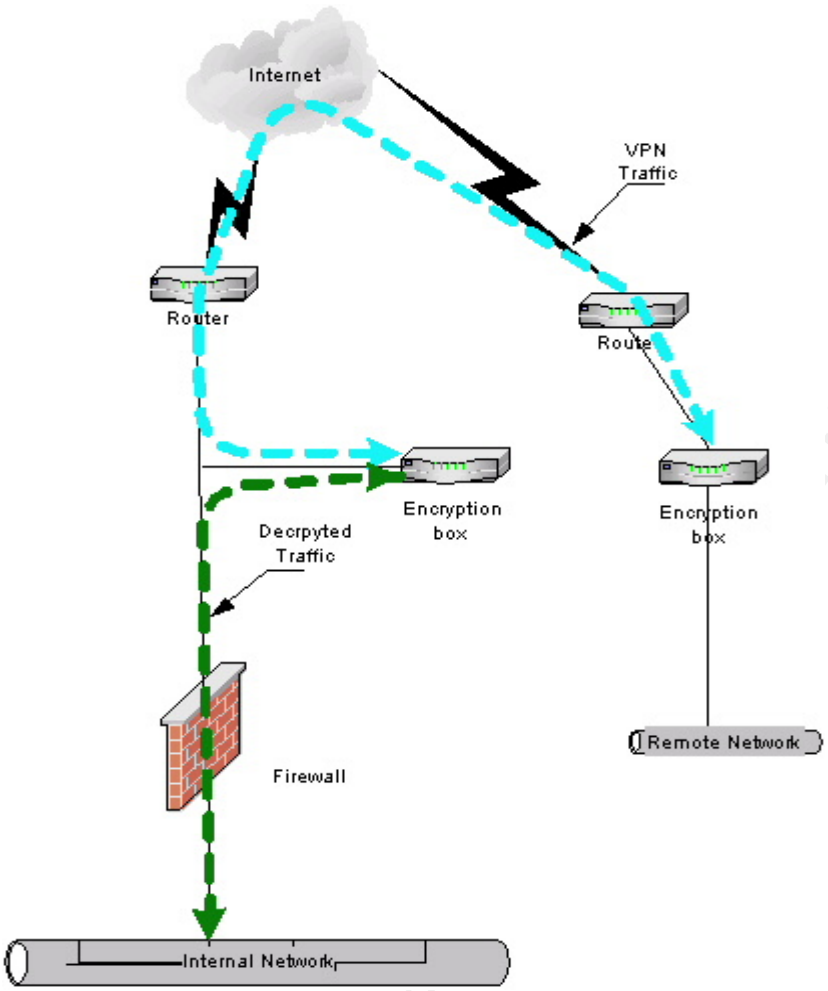

Figure3

Behind Of Firewall

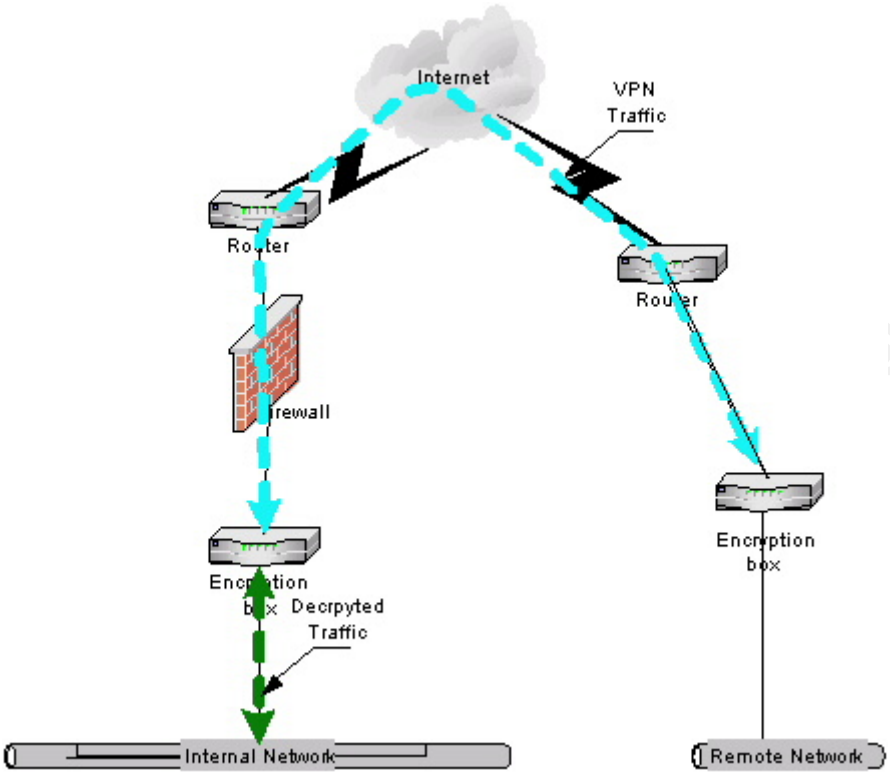

Figure4

If you install the encryption box behind of firewall, then Encryption box will be protected by firewall, but firewall can't see encrypted traffic, so firewall can't filter the traffic, just pass all encrypted traffic to the VPN box (see Figure4).

It will open big hole in firewall, hackers can pretend to be encrypted traffic to attack VPN box, if they get access to VPN box, then they can bypass firewall to do whatever they want. Also if anyone can break in remote site, they can go through VPN tunnel to break into your site, so you must have some kind of trust for the remote site. Also the remote sites must have same level of security as you have. At the solution, the level of security is decided by your firewall and your site, is decided by the weakest link of whole VPN network.

For IPSEC traffic passing through firewall, you need open two protocols (ESP, AH), one UDP port (ISAKMP), below is one example [6]of Cisco PIX firewall configuration for IPSEC traffic.

```
ip host Encryption_box 1.1.1.1
ip access-list extended Alllow-IPSEC
#Permit IP protocol 50 (ESP) through
permit 50 any host  Encryption_box
#Permit  IP protocol 51 (AH) through
```

[6] Cisco.com "Configuring the Cisco VPN 3000 Concentrator to the PIX Firewall" Nov 0 4, 2002 URL:http://www.cisco.com/warp/public/471/ALTIGA_pix.html

```
permit 51 any host Encryption_box
#Permit IKE ( UDP port 500, ISAKMP) through
permit udp any host  Encryption_box eq 500
deny ip any any
interface Ethernet0
ip access group Allow-IPSEC out
```

The example for Checkpoint Firewall,

Source	Destination	Service	Action	Track
Local VPN box	Local VPN box	ESP		
Remote VPN box	Remote VPN box	AH ISKMP	Accept	Long

In most of company, internal network normally run 100M network or more than 100M network, so if encryption box sit between firewall and internal network, encryption box must have enough throughput to handle that, otherwise will reduce whole network performance.

Another disadvantage of the solution is IPSEC don't support NAT, which mean if you want use NAT at firewall, you can't use this solution.

Routing is almost same like "encryption box in front of firewall", just for incoming traffic pass firewall first, then VPN box. For outgoing traffic, passes VPN box first, and then firewall.
The same as above, we also can stick VPN box at internal of firewall, or called " one-armed VPN behind of firewall" (see Figure 5), It will make implementation much easy, also fix encryption box throughput problem.
Same like " one-armed VPN in front of firewall", have two routing options.
But for option2, you need put one more router to handle routing issue and if remote end don't have fixed IP address, you must use option1.
Also option2 performance will be much better than option1, for option1 the maximum throughput will be less than half of the throughput of network interface card.

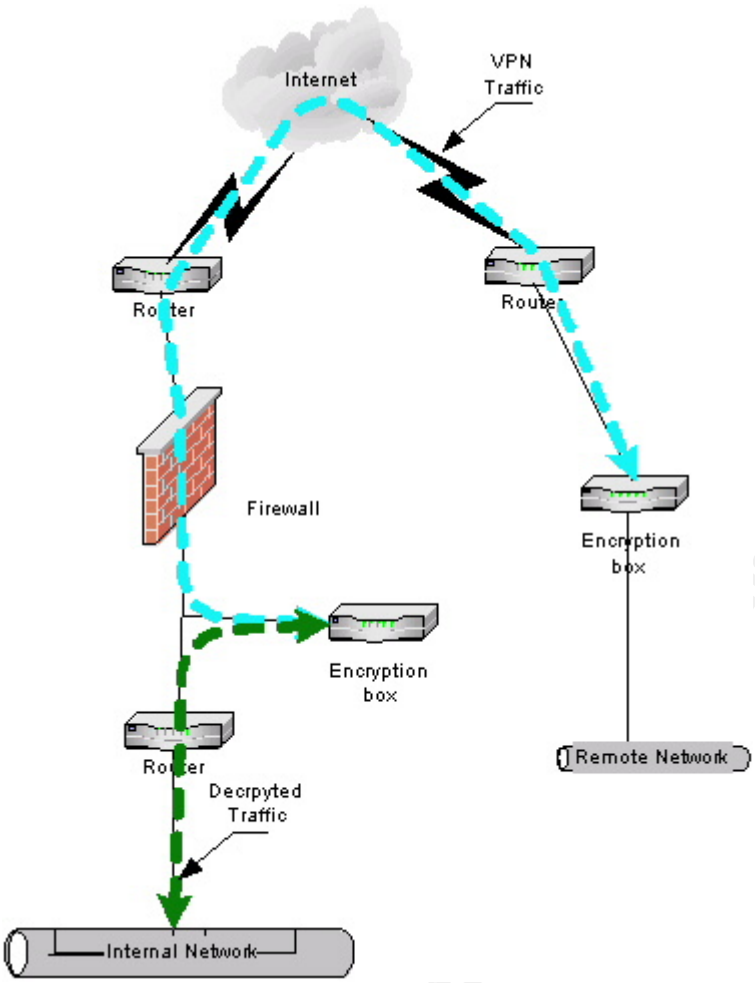

Figure5

Parallel With Firewall

VPN box Parallel with firewall (see Figure 6) is the implementation method, which is used by Cisco[7].

[7] Cisco.com " Configuring IP routing" URL: http://www.cisco.com/en/US/products/sw/secursw/ps2300/products_configuration_guide_chapter09186a008007e1ec.html#1085745

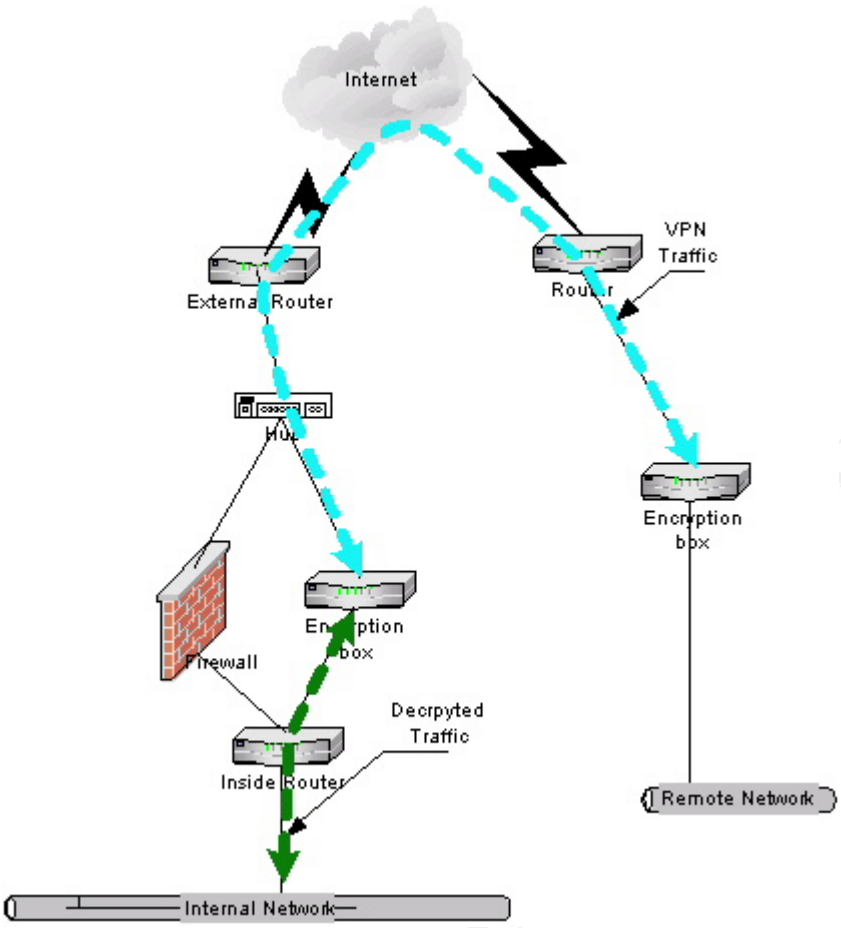

Figure 6

At the configuration, Firewall doesn't have to handle encryption traffic and unencrypted traffic at all, and VPN box doesn't need handle any other traffic. VPN and firewall is totally separated, so adding VPN box into gateway, almost don't affect the performance of firewall. And if one of VPN box and firewall is died, another one will still work, so availability is the best at all solutions.

At the configuration, you can break into internal network by cracking one of two boxes. That mean the security level of the configuration will depend on weaker one of Firewall and VPN box.

Routing will become quite complex. Normally you need put one internal router, we will discuss two options, one with internal router, one without internal router.

Option1, without internal router
For outgoing traffic, all internal hosts will put default gateway to firewall, all traffic will forwards to firewall first. At internal interface of firewall, there must be some routing table. For fixed remote VPN, route traffic to remote VPN box to local encryption box. If remote VPN don't have fixed IP address, then you can't use

this solution. Fortunately, now some VPN box support NAT or NAT Pool at internal interface of VPN box, then you can transfer all incoming VPN traffic source IP address to one range of IP addresses, which you choose, then firewall will forwards all the range of IP addresses to VPN box, VPN box will encrypt traffic and transfer destination IP address back to original IP address.

For incoming traffic, external router must be able to route incoming traffic by protocol. For encryption traffic, then route to Encryption box, the other traffic route to firewall. If external router can't route incoming traffic by protocol, you can route traffic by remote VPN IP address, but if remote VPN site don't have fixed IP address, then you cannot use that.

Option2.With internal router
If remote VPN site have fixed IP address, internal router and external router will route the traffic by remote IP address. If remote VPN site don't have fixed IP address, then internal router and external router have to route traffic by Encryption protocol. So option2 will be much simple and easy than option1, but requires one more router.

On DMZ Of Firewall

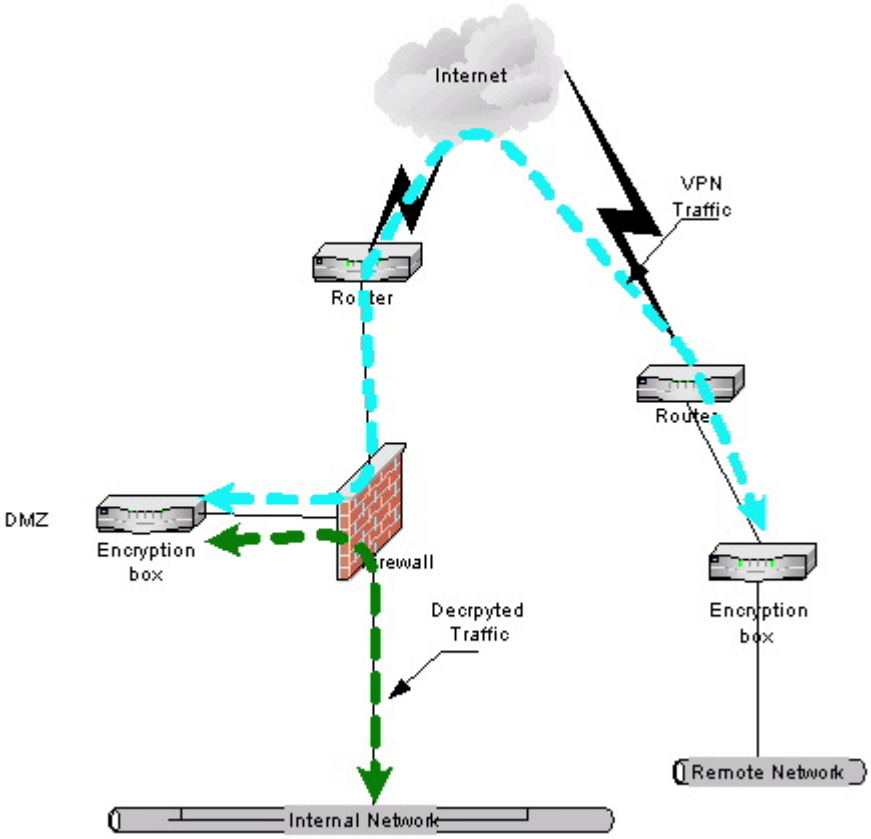

Figure 7

At the configuration (see Figure 7), VPN box is protected by firewall, and the decryption traffic also be filtered by firewall. It look like is very good solution. In fact, it has all the complexity and few of the benefits. All encryption traffic will be filtered by firewall twice, so performance is bad, and routing is nightmare. Also because of no NAT support for IPSEC, so DMZ must be legal IP address. It has all the complexity of above three solution, and benefit just have a little bit more security.

For performance, VPN traffic will be filtered by firewall twice, and firewall will handle how to route traffic. It will put a lot of load on firewall. Also same traffic transfers in same firewall DMZ interface twice, then maximum throughput is less than half of throughput of DMZ interface.

For routing, if remote site have fixed IP address, for incoming traffic, firewall can route incoming traffic by source IP address (remote VPN IP address) to VPN box, VPN box decrypts incoming traffic, then forwards to firewall, then firewall route this traffic to internal network by destination IP address. For outgoing traffic, internal network forwards all traffic to firewall, firewall will forwards to VPN box if destination IP is remote VPN IP address, after VPN encrypts the traffic, then forwards to firewall, firewall route outgoing traffic by destination IP address (remote VPN IP address). If remote VPN site don't have fixed IP address, then cannot use the solution.

Also you can put solution like Figure 8, it is as same as VPN box in front of Firewall.

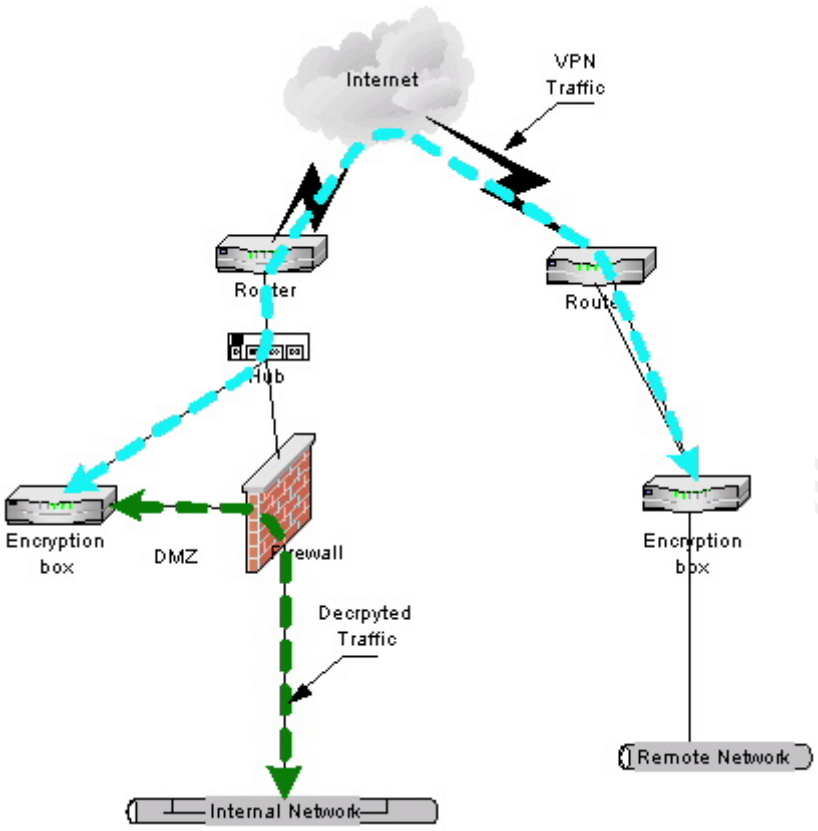

Figure 8

Or like Figure 9, it is as same as VPN box behind of firewall solution.

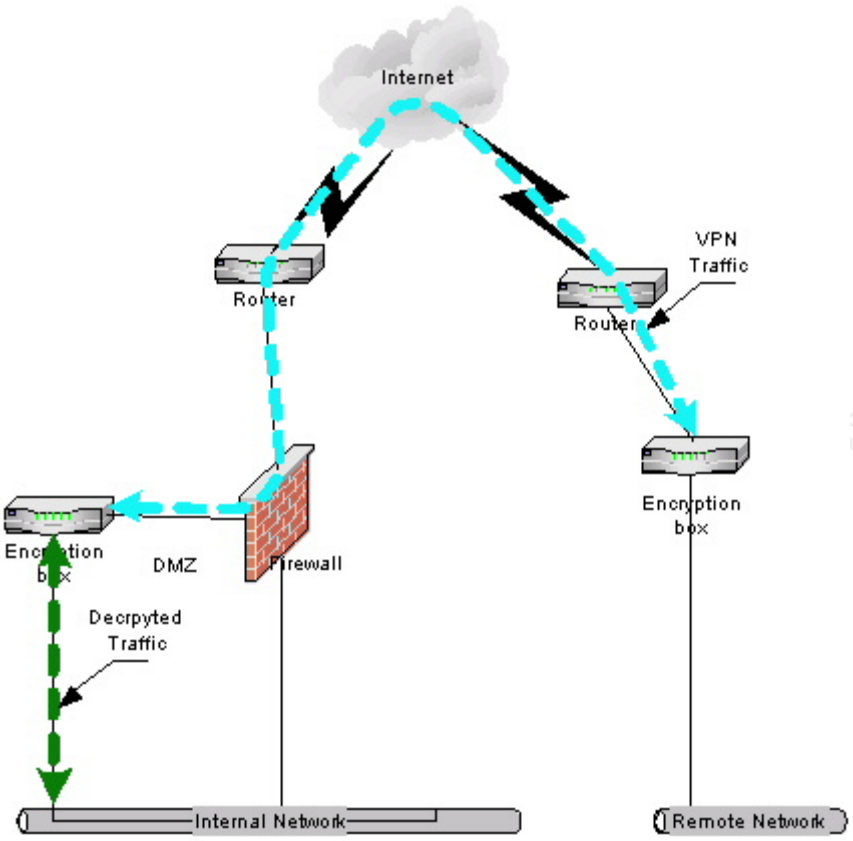

Figure 9

Hardware Encryptor With Double Layer Firewall

For double-layer firewall, naturally, you put VPN box between two firewalls (See Figure10)[8], At the configuration, for external layer firewall, you should have same consideration as VPN box behind of firewall, for internal layer firewall, should have same consideration as VPN box in front of firewall.

Unless you have security police, encryption traffic must be terminated at first layer of firewall, or you use illegal IP address at the DMZ between two firewalls. Putting VPN box in between two firewalls is an ideal solution. The outside firewall will protect VPN box, the inside firewall will filter the unencrypted traffic. But it will cost a lot because you need double your firewalls.

If you must put VPN box in front of double layers firewall, you can treat double layer firewall as one firewall, you should have same advantage and disadvantage as VPN box in front of firewall.

[8] Preston Wade "retains Case Study: Internet Firewall Architecture" Jan 13 2002 URL: http://www.giac.org/practical/GSEC/Preston_Wade_GSEC.pdf

Same for VPN box behind double layers firewall, you can treat it same like VPN box behind firewall.

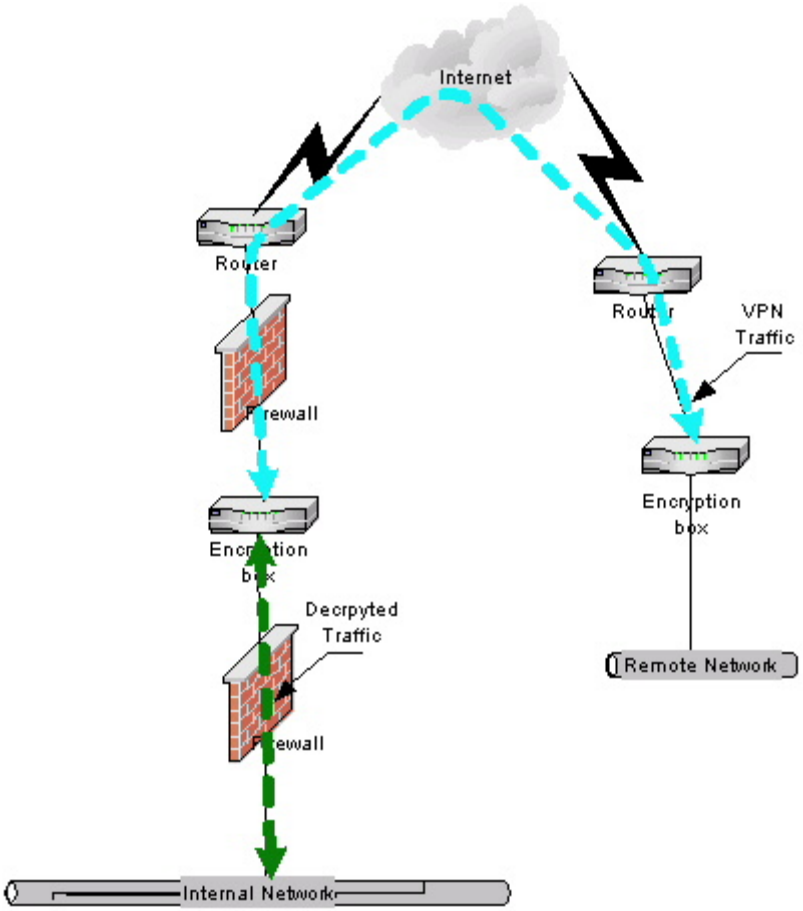

Figure 10

Recommendation

For double-layer firewalls, if you need use NAT at external firewall or corporate security requirement, you may consider to put the hardware encryption box at front of firewall, Otherwise, between two firewalls (Figure 10) will be the best solution.
Because in the case, you can protect your VPN box, also you can filter encrypted and unencrypted traffic. It is very secure. If your company already have double layer firewall, it is easy to put in and don't add any complex into your gateway system, it is ideal solution. If you must put VPN box outside of double-layer firewalls, you can treat the double-layer firewall as one firewall, then it is same like VPN box in front of firewall.

If you don't have double-layer firewalls, the security is your first priority and cost is your last priority, upgrading your whole gateway system to double layer is recommended.

But upgrading to double-layer firewalls will cost your quite a lot, and add a lot of complexity to your gateway system. Improving on security is not really a lot, because for encrypted traffic, firewall can't see that, filter or no filter don't make much different. It is not recommended to upgrading to double-layer firewalls just for VPN box, because it cost a lot, return is not much.

For no firewall at branch offices, it is recommended to use VPN box as pure VPN box (Figure1). It will cost more at traffic, but it will save some time at management of remote branches filter rule-set, and more secure. If you don't really have central office, the central office and branches offices almost are same size, it will be more economic to pass branch offices traffic locally to local ISP, just internal communication is passed through VPN tunnel. At the case, you can use VPN box as one simple firewall, but it is quite hard to mange and not secure. Maybe using firewall with VPN enabled or adding one firewall in will be one solution you should consider.

For companies have single-layer firewall, and want to add one VPN box into, it is quite complex. There are some suggestions.[9] [10] [11]

1. The best practice: Put the VPN box inside (Figure4),
   - You can protect your VPN box
   - Most of VPN box can filter traffic
   - Minimal complexity
   - Maximal performance.
2. If you want to test or quick way to implement VPN box, Sticking VPN box in front of firewall (Figure 3) or sticking VPN box behind of firewall (Figure 5).
   - You may not even have to touch your firewall at all
   - Don't need change network structure
   - Minor routing changes
3. If you have NAT or already use NAT, VPN box must be outside of firewall (Figure2).
4. If you need high availability, you may consider parallel firewall and VPN box (Figure 6), if firewall is down, you still can use VPN.
5. If you need firewall to filter packets after they have been decrypted, VPN box must be outside (Figure2), or use double-layer firewall (Figure10).

---

[9] Experts-exchange.com "VPN Design question". URL:http://www.experts-exchange.com/Hardware/Routers/Q_20138210.html

[10] Der-keiler.de "RE: VPN concentrator placement". URL: http://www.der-keiler.de/Mailing-Lists/securityfocus/security-basics/2002-09/0194.html

11 Nokia Ltd " Nokia VPN Gateway Administrator", Version 1.0 Sep 2000, Pages 15-32

6. If firewall is already over-loaded or running marginally, you may put VPN box behind of firewall (Figure4), then firewall just simply pass through IPSEC and firewall don't touch it at all. Or you can put VPN box parallel with firewall (Figure6), because firewall and VPN box is almost separated, so putting VPN box in will not affect on the firewall.
7. If you need VPN box to get your inside authentication database or certificate server, you may need to put VPN box inside of firewall (Figure 4) to authenticate.
8. If you have company security policy, all encryption traffic must be terminated at outside of firewall, then you must put VPN box outside of firewall (Figure2).

Conclusion

Adding one VPN box into your gateway, it does add more complexity to your gateway system. There are some situations I will prefer to use VPN box with Firewall.
1, you have a lot of remote users, such as mobile users or home users, need access internal network by VPN, using one VPN box just handling that kind of traffic, it will remove a lot of load from firewall.
2, if you have a lot of small branches, such as banks, using VPN boxes to connect all small branches to Data Center will be easy to implement, manage and maintain.
3, if a lot of traffic need to be passed through VPN, using VPN box will be more efficient. Because of most of hardware VPN boxes are designed to encrypt traffic.

If you are not in those situations, upgrading or enabling your firewall with VPN will be much easy and straight forwards.

For hardware VPN and firewall solutions, there is not really one solution, which will fit for all networks. All solution will have some advantages and disadvantages. The following you must consider before you make a decision, such as NAT, routing, bandwidth, network structure, security etc.

.

List Of Reference

Racal Security and Payments. “Network Security and VPN solutions” URL: http://www.parallaxresearch.com/dataclips/pub/infotech/protocols/VPN/Security_and_VPNs.PDF

Cisco.com “Cisco VPN 3000 Concentrator and Client Frequently Asked Questions” Apr 15, 2003. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_qanda_item09186a0080094cf4.shtml#Q3

Experts-exchange.com “VPN Design question”. URL:http://www.experts-exchange.com/Hardware/Routers/Q_20138210.html

Der-keiler.de “RE: VPN concentrator placement”. URL: http://www.der-keiler.de/Mailing-Lists/securityfocus/security-basics/2002-09/0194.html

Cisco.com “Configuring the Cisco VPN 3000 Concentrator to the PIX Firewall” Nov 0 4, 2002 URL:http://www.cisco.com/warp/public/471/ALTIGA_pix.html

Thales-esecurity.com “Embedded Router Encryption-AN Analysis of Security Weaknesses”. URL http://www.thales-esecurity.com/CMS/docs/encryption.pdf

Nokia Ltd “ Nokia VPN Gateway Administrator”, Version 1.0 Sep 2000, Pages 15-32

Preston Wade “retains Case Study: Internet Firewall Architecture” Jan 13 2002 URL: http://www.giac.org/practical/GSEC/Preston_Wade_GSEC.pdf

Cisco.com “ Configuring IP routing” URL: http://www.cisco.com/en/US/products/sw/secursw/ps2300/products_configuration_guide_chapter09186a008007e1ec.html#1085745

Cisco.com “Understanding the VPN 3000 Concentrator” URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_chapter09186a00800bf699.html#xtocid4