Global Information Assurance Certification Paper

IPSec and MPLS, (Even Better Together)

GIAC Security Essentials Certification (GSEC)

Practical Assignment

Option 1

File name: Gary_Biggin_GSEC.doc

Table of Contents

List of Figures

Abstract

This paper will illustrate the benefits and security features associated with deploying MPLS in a service provider's network. It will highlight some of the key components and security features (sometimes referred to as value-added services) of IPSec and MPLS VPNs and will demonstrate why MPLS VPNs are considered a "secure" means of transporting customer data. It will show that if the objective is confidentiality, IPSec will be the obvious choice, but if the objective is strictly security, MPLS VPNs will meet the customer's needs without introducing the latency associated with IPSec.

In many cases the technology choice and the value-added services chosen will depend on the level of security an organization seeks to achieve, but generally speaking, the more options (value-added services) chosen the more latency is introduced. This paper will illustrate that when deploying IPSec on MPLS, how certain IPSec value-added services may no longer be required, this is due to the inherent security features of the MPLS VPN technology. It will show that a direct result of this relationship is reduced complexity and latency in the network.

IP Security (IPSec)

Let's first look at the Security features and value-added services of IPSec.

IPSec is a set of open standards defined in RFCs 2401 and beyond that ensures secure and private communications over an IP network, the IPSec standard provides network encryption (confidentiality), digital certification (integrity), and device authentication (authentication). An IPSec tunnel is comprised of a secure link between two IPSec gateways, the IPSec gateways exchange an encryption key so the data passing between them can be encrypted. The networks behind the IPSec gateways are considered trusted and therefore data on these trusted networks is not encrypted. The IPSec gateway is responsible for ensuring that its peer gateway is the appropriate end point and is responsible for encrypting and decrypting the data.

The IPSec standard provides considerable flexibility from the users perspective. One can choose a verity of value-added services such as shared secrets with AH or digital certificates with ESP, and even a Certificate Authority (CA) if desired. One can create a single tunnel to carry all protected traffic between IPSec gateways or a separate tunnel for each TCP session. Many devices, such as Personal Computers, Servers and Firewalls support IPSec and can function as IPSec gateways, however, a number of vendors have product lines whose

primary focus is “dedicated IPSec devices”, these devices generally provide a verity of functions not available on Personal Computers, Servers and Firewalls.

The IPSec standard included many protocols but the Authentication Header (AH) and Encapsulating Security Payload (ESP) are most commonly used to provide traffic security. AH provides “**connectionless integrity**” through the use of secret-key or public-key based algorithms that allow the recipient of a piece of protected data to verify that the data has not been modified in transit. It provides “**data origin authentication**”, a security service that allows the receiver to verify that protected data could have only originated from the sender. This service requires a data integrity service plus a key distribution mechanism where a key is shared only between the sender and receiver. AH also provides an optional “**anti-replay**” service, anti-replay is a security service that allows the receiver the ability to reject old or duplicate packets in order to defeat replay attacks (replay attacks occur when the attacker sends out older or duplicate packets to the receiver and the receiver thinks that the duplicate packets are authentic). Replay-detection is accomplished by the use of sequence numbers combined with authentication. The AH is embedded in the data to be protected and can be used alone or in conjunction ESP. For more information on AH refer to RFC 2402.

The Encapsulating Security Payload (ESP), in addition to providing **connectionless integrity**, **data origin authentication**, and the **anti-replay** services that AH provide, may also provide **confidentiality** through encryption. The major difference between AH and ESP is that ESP completely encapsulates user data. ESP can be used by itself or in conjunction with AH. For more information on ESP refer to RFC 2406.

AH and ESP headers can be combined in a variety of modes. The “Security Architecture for the Internet Protocol” Document, RFC 2401, describes the combinations of security associations that must be supported.

As mentioned above, AH and ESP may be applied alone or in combination with each other to provide a desired set of security services. A direct benefit of this flexibility is that if the network is considered to be secure and confidentiality is not required, there may be no need to introduce the additional overhead of encryption provided by ESP. Both AH and ESP support Tunnel and Transport modes for datagram encapsulation. Transport mode encapsulates (protects) the upper layer payload such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) of the original IP datagram but not the IP header itself. Transport mode can only be used when the peers are the communication endpoints. Tunnel mode however, encapsulates the complete IP datagram for IPSec and is used to protect datagrams sourced from or destined to non-IPSec systems such as in a Virtual Private Network (VPN) scenario.

Another protocol commonly used in IPSec is Internet Key Exchange (IKE). IKE is a key management protocol standard which is used in conjunction with the IPSec standard. IKE is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework.

IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without manual pre-configuration. IKE eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers. It allows for the configuration of specific lifetimes for the IPSec security association, allows encryption keys to change during IPSec sessions, allows IPSec to provide anti-replay services, permits Certification Authority (CA) support for a manageable, more scalable IPSec implementations and allows for dynamic authentication of IPSec peers.

As mentioned above, IKE performs the key management function and negotiates which AH and ESP algorithm should be used, provides authentication of the IPSec peers and negotiates IPSec keys and security association. However, before an IPSec Security Association can be established and data exchanged (a process known as Phase 2), IKE must first establish a Security Association to serve as an initial secure means of exchanging keys (a process know as Phase 1). A Security Association must be established between all gateways with the encryption option and can be accomplished using “main mode” or “aggressive mode” exchange,.

Using “main mode” the first two messages negotiate the policy, the next two exchange Diffie-Hellman public values and ancillary data necessary for the exchange and the last two messages authenticate the Diffie-Hellman exchange. (The Diffie-Hellman exchange is a method to securely exchange the keys that encrypt the data. Diffe-Hellman accomplishes this secure exchange by creating a "shared secret" (sometimes called a "key encryption key") between two devices. The shared secret then encrypts the symmetric key (or "data encryption key" i.e. Data Encryption Standard (DES) and Triple-Data Encryption Standard (3DES)). Main mode uses digital certificates, pre-shared keys, and encrypted nonce. Pre-shared keys are keys installed in advance at the endpoints. Encrypted nonces involve the generation of public or private key pairs at each endpoint and the manual copying of public keys to every other endpoint.

Using “aggressive mode” the first two messages negotiate policy, exchange Diffie-Hellman public values and ancillary data necessary for the exchange and identities. The second message authenticates the responder and the third message authenticates the initiator and provides a proof of participation in the exchange. The final message may not be sent under protection of the ISAKMP SA allowing each party to postpone session establishment, (if desired) until negotiation of this exchange is complete. Aggressive Mode allows two parties to

maintain multiple, different pre-shared keys and identify the correct one for a particular exchange.

The three most common algorithms for data encryption are Data Encryption Standard (DES), Triple-Data Encryption Standard (3DES), and Advanced Encryption Standard (AES). DES was first published in 1977 by the National Bureau of Standards, it is a 56-bit secret key encryption scheme based on the Lucifer algorithm from IBM. 3DES is the **s**ame as DES except it uses a 168 bit crypto key thus provides a higher level of encryption than DES. AES, (formerly known as Rijndael), was chosen by the National Institute of Standards and Technology (NIST) as the successor to DES. AES supports three key sizes: 128 bits, 192 bits, and 256 bits but the default key size is 128 bits, all implementations MUST support the 128 bit key size. Implementations MAY also support key sizes of 192 and 256 bits. AES uses a different number of rounds for each of the defined key sizes. 128-bit key implementations MUST use 10 rounds, 192-bit implementations MUST use 12 rounds and 256-bit key implementations MUST use 14 rounds. For more information on IKE refer to RFC 2409.

Multi-Protocol Label Switching (MPLS)

Now let's look at some of the value added services and security features of MPLS VPNs:

MPLS is an Internet Engineering Task Force (IETF) specified framework that specifies methods to manage traffic flows between different devices and or applications. MPLS is protocol independent and allows for the mapping of IP addresses to MPLS labels, which are used to forward packets through the MPLS network. MPLS supports a number of the standard routing protocols such as EBGP and OSPF, and protocols that provide Quality of Service (QoS) such as resource reservation protocol (RSVP).

MPLS allows routers to reduce their processing overhead and provided new traffic engineering opportunities, MPLS also supports tunnelling and new VPN technologies. MPLS is used to forward packets over the MPLS IP backbone using the Border Gateway Protocol (BGP) for the distribution of routes. The primary focus of MPLS was to remove the overhead associated with route look-ups. As frames enter an MPLS network, a look-up is performed at the edge of the network and a label is added to the frame as it is forwarded. All router decisions in the MPLS network are accomplished by comparing the incoming MPLS label with a label forwarding table that tells the router which port to send it out and with which new label to attach. The routers at the edge of an MPLS network known as Label Edge Routers (LER) are the only ones that perform an IP address look-up, all other routers known as Label Switch Routers (LSR) make decisions based on the label-forwarding table.

In addition to removing the overhead required for route lookups, MPLS supports traffic engineering, which allows frames to be forward through the network differently based on the label parameters identified in the header. This functionality allows the Service Provider to route traffic with different priorities for different classes of service. MPLS also offered the ability to tunnel, which offers a Service Provider the means to combine many labels that are being forwarded to the same destination by placing a common tunnel label into the frame. The datagram would now have two labels, but the Label Switch Routers (LSRs) would only forward the frame based on the outer, tunnel label. Traffic engineering will introduce overhead into the network because some interjection is required for each traffic-engineered route. However, in spite of the amount of interjection required for traffic engineering, tunnelling still reduces the overhead of a traffic-engineered path by allowing one path to serve many customers.

MPLS provides new VPN technologies such as Virtual Leased Lines (VLL) and Virtual Private Networks (VPN). Virtual Leased Lines are similar to that of Leased Lines (LL) technologies such as Frame Relay (FR) and Asynchronous Transfer Mode (ATM), and like FR and ATM are generally point-to-point connections. However, a VLL is only virtual from the perspective that it emulates the leased line technology. A Label Switched Path (LSP) through an MPLS network is considered to be the same as an ATM Permanent Virtual Circuit (PVC) or FR Data-link Connection Identifier (DLCI). The header information in the datagram uniquely identifies the leased line or virtual leased line, whether this is an MPLS label, an ATM PVC, or a Frame Relay DLCI. So a leased line or virtual leased line, whether logical or not, perform the same function.

Unlike the VLL technologies that are generally point-to-point networks, VPNs are generally multi-point networks, however, both VLLs and VPNs provide separation of customer traffic. The traffic from one customer is separated from another using a unique label, the label is chosen based on the destination of the datagram, and in a multi-point network any number of destinations may be available. The Label Edge Router (LER) will decide, based on its VPN forwarding table, which is the intended destination and which label should be added to the datagram.

MPLS has a number of inherent security features that protect customer data through the network, they include address space and routing process separation to prevent the mixing of customer traffic, the prevention of label spoofing and address hiding to prevent unauthorized access and malicious attacks on the network.

Address Space and Routing Separation ensures that independent or nonintersecting VPNs within MPLS VPN service are completely independent of each other, meaning each can use the same address space, both on the VPN and in the core. Routing between VPNs is completely independent and routing between the VPNs and the core is also completely independent. The primary reason for this unique independent separation of addresses and routing

processes is to ensure that a packet destined to a host on one VPN is not accidentally routed to a host in another VPN with the same IP address.

Hiding of the MPLS Core Structure ensures that the Provide Edge (PE) and Provider (P) router's addressing and routing structure is not visible to outside networks such as another VPN or the Internet. One of the benefits of doing so is that denial-of-service attacks against a core router are more difficult if the attacker does not know the IP address structure, if the addresses are not known the attacker will have to guess the address before an attack can occur. In an ideal scenario, the MPLS core should be as invisible to the outside world as a traditional layer two infrastructure such as Frame Relay or ATM.

The two most common types of attacks on IP networks are unauthorized access or intrusions and Denial of Service (DoS) attacks. For the first, (unauthorized access), the best means of protection is to harden protocols such as Telnet access to routers and to make the network as inaccessible as possible using a combination of packet filtering or use of firewalls and address hiding, as discussed above. For the second, (DoS attacks), the only way to be certain the network is not susceptible to this kind of attack is to make sure that machines are not reachable, again by packet filtering and address hiding.

Impossibility of Label Spoofing limits the ability of an attacker to spoof an IP address and making the address appear as though it belongs to them. In a pure IP network, it is easy to spoof IP addresses, but because MPLS uses labels instead of IP addresses the likelihood of this happening in a MPLS VPN network is reduced. Assuming proper configuration to achieve address and routing separation as discussed above, spoofing a MPLS label is not possible. A PE router should never accept a packet with a label from a CE router because CE routers do not participate in the distribution of MPLS labels. In Cisco routers, the implementation is such that packets that arrive on a CE interface with a label will be dropped, thus it is not possible to insert fake labels because no labels are accepted. That being said, the only other possibility is to spoof the IP address of a packet that is being sent to the MPLS core. However, because of the strict address separation within the PE router, and each VPN having its own VRF, this can harm only the VPN that the spoofed packet originated from, thus VPN customers can only attack themselves.

MPLS is defined in RFC: 2547 and an overview on Securing the MPLS Architecture is discussed in a Cisco white paper "Security of the MPLS Architecture" at http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mxinf_ds.htm

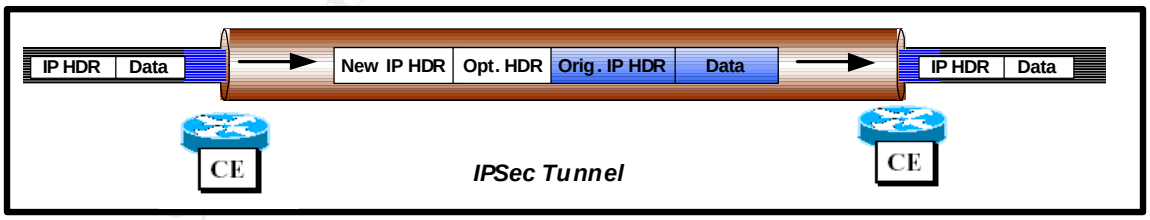
IPSec and MPLS

The paper will now look at how IPSec and MPLS may be combined to effectively deliver Network based IPSec services. If it's determined that confidentiality (encryption) is required, there are a number of implementation options and vendor's equipment to choose from. As mentioned before, IPSec gateways can be Personal Computers (PCs), servers, routers, firewalls, or dedicated IPSec security devices. IPSec tunnels can be established between many combinations of IPSec gateways but with any combination there is potential for vendor incompatibilities. Vendor interoperability is always a consideration when configuring IPSec between different vendor's equipment.

In addition to the potential for vendor and gateway incompatibilities, when deploying IPSec, one must also consider the management and support components. Incorrect configurations can be detrimental and one needs to consider carefully which security services will be used and in what combinations.

So given the potential for vendor incompatibility and incorrect IPSec configurations it seems reasonable that standardizing IPSec gateways and automating processes where possible would be considered good practices. The following sections will illustrate how IPSec can be implemented on a MPLS network leveraging existing CE routers as the IPSec gateways as an alternative to deploying host or applications based IPSec. These sections will also show the advantages of deploying IPSec in combination with MPLS.

The following diagram is a logical representation of how CE routers are used as IPSec gateways and how data passing between them is encrypted and un-encrypted at the network edge.



IPSec between CE routers

Implementing network based IPSec on a MPLS VPN network is usually done on the Customer Edge (CE) router. This IP encryption option is commonly defined as a routed link between two or more sites across the VPN network topology that ensures confidentiality for all parties. The fundamental reason for using this encryption feature is to offer more secure data transmission over the already secure MPLS VPN network via the added confidentiality and integrity of IPSec.

As mentioned above, network based IPSec implementations are becoming an attractive alternative to hosts and applications IPSec tunnels, especially in cases where these network devices already exist. Deploying IPSec on existing equipment reduces the cost and complexities of having to deploy addition equipment thus reducing the equipment footprint, power and environmental consideration and additional training and support issue. In many cases there will be additional costs associated with adding a hardware acceleration module to the network device but the footprint, power and environmental requirements will remain the same.

Network based IPSec devices provide the ability to dynamically establish IPSec tunnels and reduces the number of point-to-point connections between hosts and applications. The CE router can be configured to encrypt traffic from a verity of hosts or an application depending on the requirement. IPSec handles encryption by using a gateway-to-gateway or CE-to-CE router approach to create an overlay encrypted network (IPSec VPN) on top of the (MPLS VPN) network in a mesh or hub-spoke topology. IPSec requires each CE to route data identified to be encrypted through the VPN service in a virtual tunnel that both verifies the authenticity of the parties at both endpoints and encrypts the data. The tunnels can be established statically or dynamically and can include the entire Virtual Routing and Forwarding table (VRF) or specific host addresses in the VRF. Deploying IPSec on the CE Router can help reduce latency in the network because most of the processing required for encryption can be done in hardware. Cisco routers use an Accelerator Integrated Module (AIM) to perform this function. Lower latency could be significant if the Service Provider has contractual obligations for throughput.

When the Service Provider owns and operates a Network based data encryption service the encrypting gateways are located in the provider network. Network-based solutions allow the provider to offer encryption services to multiple customers using a single gateway such as a router, and one of the advantages of deploying IPSec on MPLS is that since the MPLS VPN service is much more secure than the Internet, there is no need to use all the value-added-feature provided by the IPSec standard such as the use of digital certificate and ESP.

For many customers in a MPLS network scenario, shared secrets will be considered sufficient due to the inherent security features of MPLS VPNs, the ability to use “shared secrets” eliminates the costs and complexities associated with digital certificates and implementing a Certificate Authority (CA). And for many customers AH is sufficient protection for data when IPSec is deployed on MPLS, thus eliminating the overhead of ESP. Remember, AH and ESP both provide connectionless integrity, data origin authentication, and anti-replay services but ESP also allows for the complete encapsulation of the user data if required. However, as mention before this value-added feature introduces additional latency. The key is to understand the requirement. If the network is

already secure and confidentially is not a concern, encapsulation of the users data may simply add unnecessary overhead.

There is a verity of ways to identify traffic that should be encrypted but this paper will focus on the Cisco CE router implementation in a MPLS VPN scenario. IPSec tunnels can be configured manually or dynamically. Manual configurations may be acceptable in very small networks but are not suitable for larger enterprise networks. Cisco uses Tunnel Endpoint Discovery (TED) to dynamically identify traffic to be encrypted. TED allows dynamic Crypto Map entries on the CE's to reduce the amount of configuration and maintenance required for an IPSec implementation. TED can be used to dynamically establish tunnels based on Interesting traffic thus reducing the need to manually configure tunnels through the network. Interesting traffic is the traffic that the user wishes to encrypt, it can be defined using source and destination IP addresses or the port numbers of the applications, using IP addresses and port numbers can reduce the size of the interesting traffic definition and therefore the effort required to manage it.

A Crypto Map is used to define the traffic that should be encrypted. "Crypto MAP", is a Cisco IOS software configuration entity that selects data flows that need security processing and defines the policy for these flows and the crypto peer to which the traffic needs to go. The crypto map is applied to a network device's interface.

Without TED, all CE's participating in IPSec communications with each other must have static configuration to establish the IPSec tunnels. Using TED, interesting traffic (traffic to be encrypted) must still be defined (in an Access List), but if the Security Association has been confirmed, the CE will automatically establish a tunnel with an un-known end point when it receives interesting traffic to send across the WAN. The stipulation is that the CE on the other end of the tunnel shares the same encryption parameters and pre-shared keys as the side initiating the tunnel.

For more information on TED see Configuring IPSec Tunnel End-Point Discovery http://www.cisco.com/warp/public/707/tedpreshare.html

Summary

The paper has looked at some of the value-added services and security features of IPSec and MPLS VPNs, it has established that MPLS VPNs are not a replacement for IPSec because it does not provide confidentially and integrity, IPSec provides encryption and MPLS VPNs do not. However, we have also established that if the primary goal is to achieve security and not confidentiality, MPLS VPNs will be a valid option and will result in optimal communications due to lower latency in the network.

IPSec is the obvious protocol of choice when it comes to information security and when using the public Internet there are very few practical alternatives. However, as MPLS VPNs become more prevalent we must stop and consider the security benefits associated with this technology. We have established that MPLS VPNs are secure, they employ a number of security features that eliminate the major vulnerabilities associated with the public Internet and as a direct result eliminate some of the security requirements associated with these vulnerabilities.

The paper has also shown that when IPSec is deployed on a MPLS VPN network that some of the valued added services in the IPSec standard (such as digital certificates and ESP) may no longer be required, this due to the inherent security features of MPLS VPNs. The paper has also shown that deploying IPSec on the CE routers at the network's edge may reduce the complexities of vendor interoperability while providing a very scalable, manageable and affordable IPSec service.

Terminology

Authentication Header (AH): A security protocol that provides that provides "connectionless integrity", "data origin authentication", and an optional "anti-replay" service AH is embedded in the data to be protected (a full IP datagram, for example). AH can be used by itself or with Encryption Service Payload (ESP).

Crypto Map: A Cisco IOS software configuration entity that selects data flows using an Access List (ACL) that need security processing, defines the policy for these flows and the crypto peer that traffic needs to go to. A crypto map is applied to a device interface.

Data Integrity: Through the use of secret-key or public-key based algorithms, allow the recipient of a piece of protected data to verify that the data has not been modified in transit.

Data Confidentiality: A method that changes the structure of the data to be protected using encryption and keys that are only available to the parties involved in the communication so that only the intended recipient can read it.

Data Origin Authentication: A security service where the receiver can verify that protected data could have originated only from the sender. This service requires a data integrity service plus a key distribution mechanism, where a secret key is shared only between the sender and receiver.

Data Encryption Standard (DES): The National Bureau of Standards published The DES in 1977 and is a 56-bit secret key encryption scheme based on the Lucifer algorithm from IBM.

3DES: Similar to the DES protocol except it uses a 168 bits crypto key.

Encapsulating Security Payload (ESP): A security protocol that provides data confidentiality and protection with optional authentication and replay-detection services. ESP completely encapsulates user data. ESP can be used either by itself or in conjunction with AH.

Internet Key Exchange (IKE): IKE is a key management protocol standard which is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration within the IPSec standard. IKE is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE is used to establish a shared security policy and authenticated keys for services that require keys. Before any IPSec traffic can be passed, each router/firewall/host must be able to verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.

Internet Security Association and Key Management Protocol (ISAKMP): Is a protocol framework that defines the mechanics of implementing a key exchange protocol and negotiation of a security policy.

Replay-detection: Is a security service that allows the receiver the ability to reject old or duplicate packets in order to defeat replay attacks. Replay attacks occur when the attacker sends out older or duplicate packets to the receiver and the receiver thinks that the duplicate packets are authentic.

Transport Mode: An encapsulation mode for AH and ESP, it encapsulates the upper layer payload such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) of the original IP datagram but not the IP Header itself.

Tunnel Mode: Encapsulation of the complete IP datagram for IPSec, it is used to protect datagrams sourced from or destined to non-IPSec systems such as in a Virtual Private Network (VPN) scenario.

References

The Internet proved to be a very valuable resource while doing research for this paper but the following sites were of particular interest: Special thanks to those who contributed to these papers.

The Internet Engineering Task Force home page
http://www.ietf.org/
The Internet Engineering Task Force Search Engine
http://search.ietf.org/

The Internet Engineering Task Force RFC page
http://www.ietf.org/rfc.html
MPLS and IPSec: A Misunderstood Relationship, Jon Ranger
http://www.riverstonenet.com/technology/mpls_ipsec.shtml
Security of the MPLS Architecture
http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mxinf_ds.htm
IPSec components overview
http://www.ietf.org/ids.by.wg/ipsec.html
A comprehensive discussion of VPN technology
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm
VPN FAQ
http://www.zyxel.com/support/supportnote/zywall10/faq/vpn_faq.htm
Configuring IPSec Tunnel End-Point Discovery
http://www.cisco.com/warp/public/707/tedpreshare.html
Configuring IPSec - Router to PIX
http://www.cisco.com/warp/public/110/39.html
Configuring IPSec Router-to-Router Fully Meshed
http://www.cisco.com/warp/public/707/ios_meshed.html
An Introduction to IP Security (IPSec) Encryption
http://www.cisco.com/warp/public/105/IPSECpart1.html
Configuring Internet Key Exchange Security Protocol
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt4/scdike.htm
Configuring IPSec Tunnel End-point Discovery
http://www.cisco.com/warp/public/707/tedpreshare.html

RFCs:
2547, BGP/MPLS VPNs
http://www.ietf.org/rfc/rfc2547.txt?number=2547
2401, Security Architecture for IP
http://www.ietf.org/rfc/rfc2401.txt?number=2401
2402, Encryption Service Payload (ESP). Refer to the
http://www.ietf.org/rfc/rfc2402.txt?number=2402

2403, The Use of HMAC-MD5-96 within ESP and AH
http://www.ietf.org/rfc/rfc2403.txt?number=2403
2404, The Use of HMAC-SHA-1-96 within ESP and AH
http://www.ietf.org/rfc/rfc2404.txt?number=2404
2405, The ESP DES-CBC Cipher Algorithm With Explicit IV
http://www.ietf.org/rfc/rfc2405.txt?number=2405
2406, Authentication Header (AH)
http://www.ietf.org/rfc/rfc2406.txt?number=2406
2407, The Internet IP Security Domain of Interpretation for ISAKMP
http://www.ietf.org/rfc/rfc2407.txt?number=2407
2408, Internet Security Association and Key Management Protocol (ISAKMP)

http://www.ietf.org/rfc/rfc2408.txt?number=2408
2409, Internet Key Exchange (IKE):
http://www.ietf.org/rfc/rfc2409.txt?number=2409
2410, The NULL Encryption Algorithm and Its Use With IPsec
http://www.ietf.org/rfc/rfc2410.txt?number=2410
2411, IP Security Document Roadmap
http://www.ietf.org/rfc/rfc2410.txt?number=2410
2412, The OAKLEY Key Determination Protocol
http://www.ietf.org/rfc/rfc2412.txt?number=2412