Universidade Estadual de Campinas
Unicamp

IPSec
Segurança de Redes – INF542

Prof. Dr. Paulo Licio de Geus
Alunos: Luis Fernando B Braghetto
Sirlei Cristina da Silva
Luis Alberto M. Barbosa
Pós Graduação em Redes Computadores

Capítulo 1 – Introdução ao IPSec

1.1 – Motivação

A cada dia a Internet está menos segura e cada vez sendo mais usada para uso corporativo.

Existem inúmeros tipos de ataques, incluindo o *eyesdropping* que na verdade é o uso de um sniffer ou algo semelhante para podermos "enxergar" o tráfego entre duas máquinas para capturar algo importante, desde senhas, dados bancários, cartões de crédito até mesmo segredos industriais.

Então houve o desejo de conectar duas ou mais empresas de maneira segura. Instalar uma rede privada pode ser fácil em duas empresas vizinhas, porém quando existem matriz, filiais, escritórios e parceiros separados por centenas de quilômetros de distância isto pode ser muito difícil. A maneira ideal seria usando uma rede pública, como a Internet, porém compromete-se fortemente a segurança.

O uso de protocolos de rede que provejam segurança da comunicação tornam-se importantes na implementação de novos recursos tais como B2B, Intranets, Extranet, etc.

VPNs (Redes Privadas Virtuais - *Virtual Private Networks*) provêm conexão segura entre duas hosts ou duas redes, permitindo que conexões privadas sejam estabelecidas usando redes públicas, tais como a Internet. A VPN é responsável por prover o apoio da rede para executar as tarefas de sigilo (criptografia), autenticação, assinatura e verificação dos segmentos, etc. Além disso é possível obter economia usando alguns recursos centralizadamente e o acesso através desta conexão, tais como servidores de banco de dados, Servidores de Intranets, etc

1.2 – Introdução a VPNs

Podemos definir uma VPN como uma emulação de uma rede de longa distância usando redes IP, tais como Internet ou podem ser visas como redes virtuais operando sobre redes reais. Entre os fatores que podemos citar estão a redução de custos, capilaridade da Internet, proteção do tráfego e fácil instalação. O tráfego da VPN não pode ter vazamentos de pacotes por fora do "túnel" criado para a VPN, como por exemplo os pacotes sinalização.

Porém a vantagem de incluir novos recursos, também traz alguns itens a se preocupar com relação à proteção da segurança, especialmente dos clientes. Estas desvantagens serão vistas posteriormente.

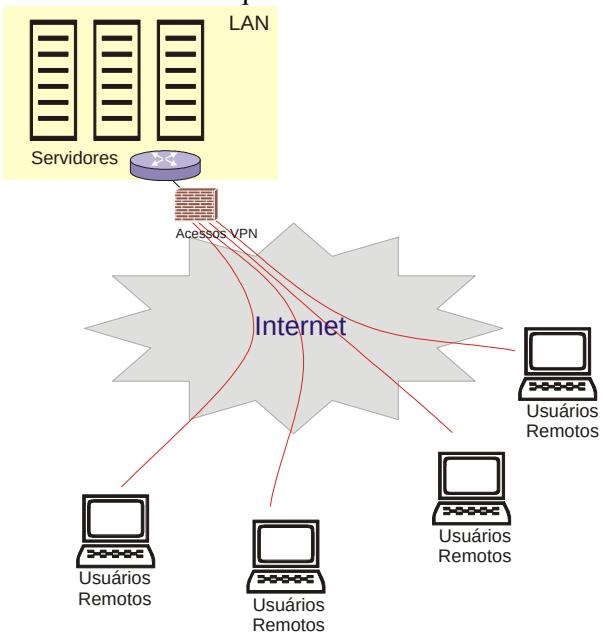
1.2.1 Tipos de VPNs:

Existem 3 tipos de VPNs:

- Remote-Access VPNs
- Site-to-Site VPNs
- Extranet VPNs

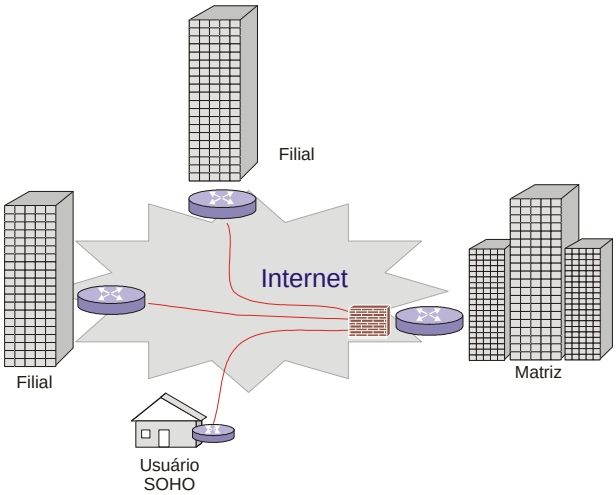
1.2.1.1 – RemoteAccess VPNs

Neste tipo de VPN, o cliente usa um software que permite conectar-se a um servidor de VPN na rede a qual deseja ter acesso. O servidor irá autenticá-lo antes de permitir que o cliente se conecte através desta conexão que será estabelecida.



1.2.1.2 – Site-to-Site VPNs

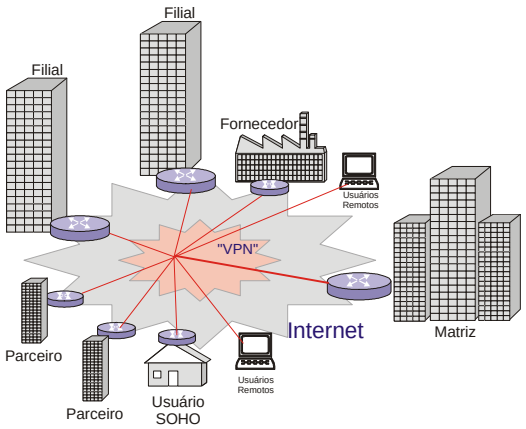
Quando duas empresas se conectam através de “gateways” de conexão, sendo assim duas redes distintas são conectadas entre si de maneira segura. Servidores, Roteadores ou equipamentos especializados se responsabilizam por autenticar-se entre si, criar o túnel, rotear pacotes, etc.



VPNs do tipo Site-to-Site são uma alternativa para conectar todas as filiais com a matriz, e ainda poder conectar eventuais parceiros a uma única rede.

1.2.1.3 – Extranet VPNs

Extranet VPNs conectam consumidores, fornecedores, parceiros e funcionários na Intranet corporativa através das conexões feitas pela rede pública através de gateways VPNs e clientes de VPNs.



1.3 – IPSec

A atual pilha do TCP/IP que está hoje em uso em todo o planeta é a versão 4. O IPv4 não possui nenhuma característica de proteção ou segurança inerente. No inicio da Internet, a privacidade não era tão vital quanto é hoje.

Os primeiros esforços de padronização (RFC1825/1829) para IP com segurança, autenticação e cifragem de datagramas foram escritos em 1995.

Na verdade o IPSec foi a resposta para a falta de segurança do IPv4, e o IPSec atualmente é o protocolo mais usado porque possui uma estrutura completa para VPNs. Este protocolo está sendo adotado a cada vez por mais fabricantes, tornando-se um padrão “de facto”.

Foram definidos dois cabeçalhos para o IPSec, o de autenticação (AH) e o de encapsulamento de segurança de carga útil (ESP) que provê o ciframento do conteúdo da mensagem.

Durante o estabelecimento da conexão, o IPSec cria um túnel. Este túnel é uma conexão especial entre dois hosts. Os gateways são responsáveis por cifrar o pacote original, adicionando um novo cabeçalho IP ao pacote. No gateway de destino, este remove os dados do pacote IP recebido e decifra e repassa à rede local.

1.3.1 – Características do IPSec

IPSec usa dois diferentes protocolos (AH e ESP) para garantir a autenticação, integridade, sigilo da comunicação. Ele pode proteger o datagrama IP inteiro ou apenas os protocolos superiores (protocolos de transporte).

1.3.2 – Modos de Operação

Os modos possíveis são o modo túnel e o modo transporte.

No modo transporte apenas o payload do datagrama IP é gerenciado pelo IPSec, ou seja, após a adição de um cabeçalho IPSec logo após o cabeçalho IP original, de modo que apenas os protocolos superiores podem ser cifrados/autenticados.

No modo túnel o datagrama inteiro incluindo cabeçalhos são cifrados e um novo cabeçalho IP é criado. Isto permite "escondermos" o endereço IP de origem e destino originais, impedindo a alteração ou conhecimento do atacante das partes envolvidas.

Um item interessante é que com o IPSec pode trafegar apenas IP unicast. Para IP multicast ou multiprotocolos deve-se usar o L2TP (Layer 2 Tunneling Protocol) em caso de VPNs do tipo RemoteAccess VPNs, porque muitas vezes o próprio tráfego já é PPP e usar o GRE (Generic Routing Encapsulation) para VPNs site-to-site.

Capítulo 2 – IPSec

2.1 – Introdução

Como já visto, o IPSec provê apoio para VPN sobre IP.

O IPSec possui três componentes:

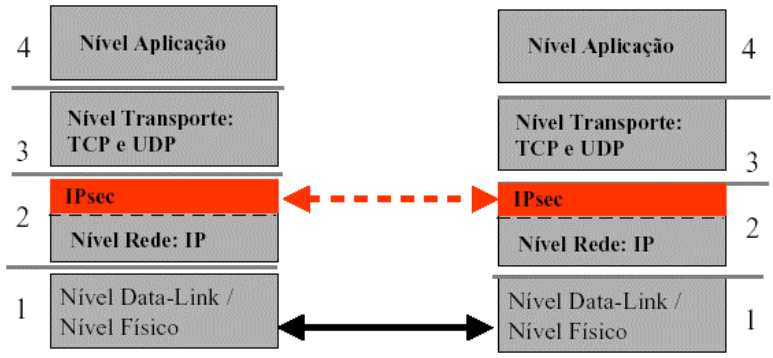
- AH (Authentication Header): fornece serviço de autenticação do pacote IP.
- ESP (Encapsulating Security Payload): fornece cifragem dos datagramas, autenticação das partes e integridade dos pacotes.
- IKE (Internet Key Exchange): negocia parâmetros da conexão, tais como chaves de sessão.

O IPSec provê uma numerosa quantidade de itens de segurança tais como criptografia (sigilo), autenticação dos equipamentos e credenciais de usuário, integridade de dados, sigilo dos endereços (*address hiding*), estabelecimento de chaves e algoritmos de ciframento.

Também deve-se ter em vista que o uso do algoritmo DES (antigo padrão de ciframento simétrico de 56 bits) é muito pouco, pois em 1999 uma competição quebrou a chave do DES em menos de 23hs. Atualmente recomenda-se o 3DES (168bits) e para integridade dos dados o uso de assinaturas MD5-HMAC (128 bits) ou MD5-SHA1 (160bits).

Entretanto o uso de criptografia mais forte significa o aumento do overhead de processamento.

O IPSec é uma camada virtual entre as camadas 2 e 3 (rede e transporte) do modelo Internet.



2.2 – Protocolos Criptográficos

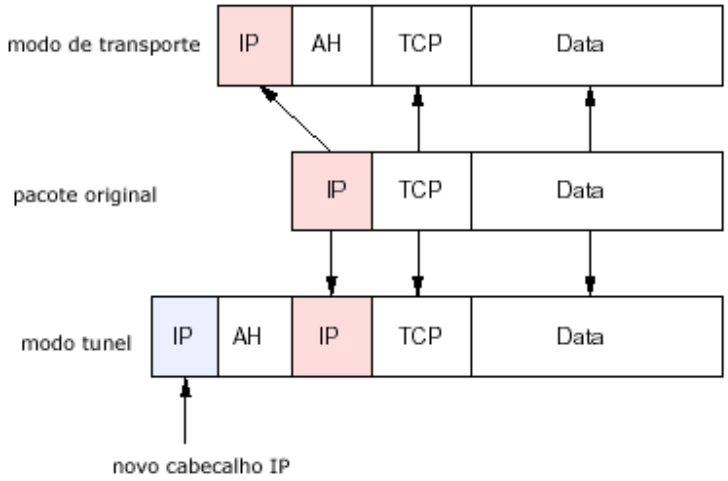
O IPSec foi construído baseados nos atuam modelos de criptografia moderna:

- Protocolo Diffie-Hellman para troca de senha secreta entre duas partes quaisquer pela rede pública
- Criptografia de chave pública para assinar as trocas pelo Diffie-Helmman para garantir a identidade das partes e evitar o ataque “man-in-the-middle”.
- DES, 3DES para criptografia simétrica (privacidade)

- Algoritmos de integridade do datagrama (hash) como MD5, SHA1.
- Certificadora digital para validação das chaves públicas.

2.3 – Formatos dos Cabeçalhos

Vejamos agora como são formados os cabeçalhos do IPSec. Lembrando que eles são levemente diferente dependendo do modo de operação: túnel ou transporte.



2.3.1 – Arquitetura de segurança do IP

Baseado na RFC2401, aqui teremos uma idéia geral de como tudo funciona. Como já dito, ele pode trabalhar como cliente/servidor (RemoteAccess VPN) ou através de gateways (Site-to-Site VPN). A proteção oferecida é baseada nos requerimentos definidos por um banco de dados de políticas de segurança (SPD – Security Policy Database).

O IPSec prove segurança e negocia os algoritmos usados para os serviços de túneis providos às camadas superiores. Ele também protege os vários caminhos entre todos os clientes individualmente. Os serviços providos por IPSec, segundo a RFC são o controle de acesso (AH+ESP), autenticação da origem do pacote(AH), integridade sem conexão (AH), integridade de seqüência (rejeição a pacotes repetidos) (AH), confidencialidade(ESP) e é possível a negociação de compressão de dados.

2.3.1.1 – Implementação do IPSec

As aplicações atuais que querem utilizar o IPSEC devem incluir pilhas especiais. A medida que mais e mais redes mudarem para IPv6, o uso destas diminuirá. Há várias formas de implementação para o IPSec, desde o servidor, até roteadores ou firewalls. Os tipos mais freqüentes são:

- Integração do IPSec na implementação nativa da pilha TCP/IP. Isto requer acesso ao código fonte e pode ser implementado tanto em servidores como gateways de segurança.
- Implementação chamada Bump-in-The-Stack (BITS) onde o IPSec é implementado sobre a pilha TCP/IP existente, entre a camada IP nativa e o

driver de rede local. Acesso ao código fonte neste caso não é necessário, fazendo dessa implementação o tipo ideal para sistemas legados. Isto normalmente é usado em servidores.

- Implementação chamada Bump-In-The-Wire (BITW), quando se faz uso de um processador dedicado à criptografia e é usado em sistemas militares e em sistemas comerciais dedicados. Essa implementação pode ser escolhida para servidores ou roteadores (gateways de VPN). Normalmente o dispositivo BITW possui um endereço IP. Quando suporta apenas 1 host, ele é análogo ao BITS, e quando implementado em um gateway de VPN ele deve operar como gateway de segurança.

2.3.1.2 – Security Association - SA

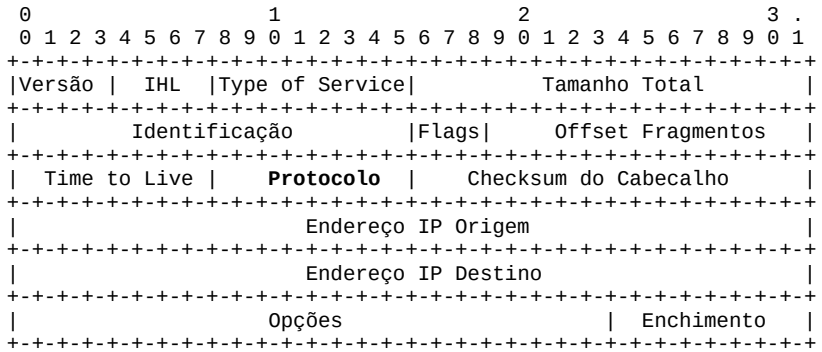
Outro conceito importante é a associação de segurança (SA - *Security Association*). O AH e o ESP usam os SAs e a principal função do IKE é estabelecer e manter o SA. Uma associação de segurança é um acordo entre entidades sobre como elas transmitirão informações de segurança. Um Security Association (SA) também pode ser definido como uma conexão simples que provê serviços de segurança para o trafego. Os serviços de segurança são certos recursos disponíveis para um AS para uso do AH ou ESP, mas não ambos. Um SA oficialmente é definido por uma tríplice de SPI, Endereço IP de Destino e Protocolo (ESP ou AH), e o SPI funciona como uma porta no TCP ou UDP para reconhecimento quando múltiplos tráfegos acontecem em um único endereço de destino.

Deve ser em mente que uma comunicação bidirecional entre hosts necessita de duas associações de tráfego (SA). Como AH e ESP não podem estar simultaneamente usando o mesmo SA, e as vezes integridade e confidencialidade são imprescindíveis precisa-se combinar SAs. Isto é chamado de "*SA bundle*".

Após um AS ser negociado, ele será incluído em um banco de dados de associações de segurança (SAD – Security Association Database). Isto é necessário porque cada conexão possui características diferentes, algoritmos, etc.

2.3.2 – Cabeçalho IP

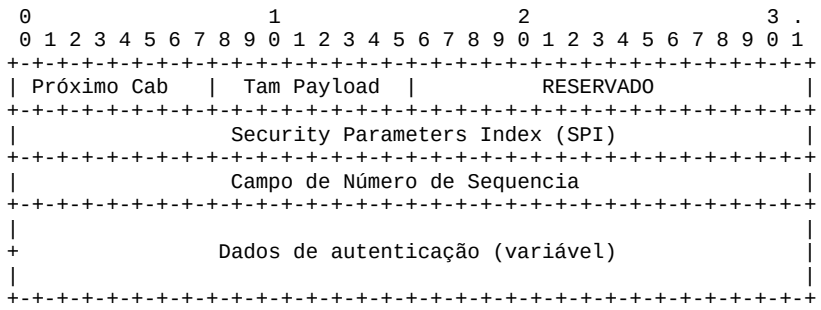
O cabeçalho IP precisa ser revisto para que mostremos onde o AH e o ESP entrarão no formato final do pacote.



O IP possui um campo chamado “protocolo” e é exatamente neste ponto que o ESP e o AH entram. O ESP é 50 e o AH é o protocolo 51, ou seja, quando esse valor é colocado no campo protocolo, na área de dados do IP seguirá um novo pacote AH ou ESP.

2.3.2 - Cabeçalho AH

O Cabeçalho AH tem várias funções conforme visto. Para implementar todas as suas funções, veremos o formato do cabeçalho do pacote de Autenticação



Vejamos os itens do cabeçalho dos pacotes AH:

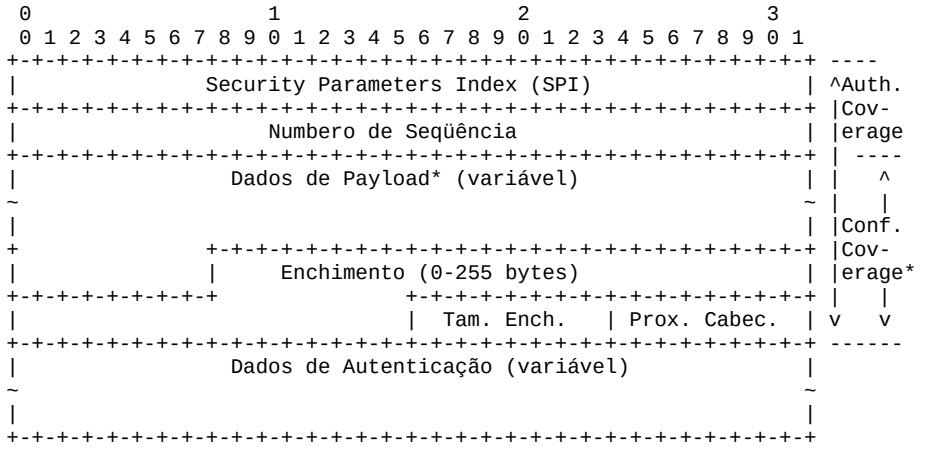
- Próximo Cabeçalho: Um valor inteiro de 8 bits que identifica o que estará presente na parte de dados após os “Dados de Autenticação”. É o mesmo valor definido pela IANA para os protocolos, exatamente igual ao IP.
- Tamanho do Payload: Valor inteiro de 8 bits que especifica o tamanho do AH em palavras de 32-bits, menos 2 (devido a compatibilidade do IPv6[1]). Normalmente são 96-bits de valor de autenticação, mais 3 palavras de 32-bits da parte fixa, então o tamanho será 4.
- Security Parameters Index (SPI): É um valor de 32-bits do identificador único que inclui o protocolo (AH) e endereço de destino, formando o identificador SA.
- Número de Seqüência: Este valor de 32-bits sem sinal contém um valor incremental do valor do número de seqüência (semelhante ao TCP). Isto faz a propriedade de anti-replay do AH.
- Dados de autenticação: Este campo de valor variável contém o valor de integridade (ICV – *Integrity Check Value*). Um enchimento (padding) deve ser usado para que o pacote tenha tamanho múltiplo de 32-bit (IPv4) ou 64-bits (IPv6). Este algoritmo usado no ICV deve ser um hash criptográfico, tais como MD5 ou SHA1 ou então uma MAC baseada em algum algoritmo como DES (pouco usado). Isto é definido pela SA.

[1] Veja RFC2402 item 2.2 e RFC1883.

2.3.3 – Cabeçalho ESP

O cabeçalho ESP (Encapsulating Security Payload) é desenhado para prover uma união entre serviços de IPv4 e IPv6. O ESP pode ser usado sozinho ou em conjunto com o AH. O ESP deve ser inserido depois do IP e antes do cabeçalho do protocolo superior (transporte) ou antes do cabeçalho IP encapsulado (modo túnel). O ESP provê confidencialidade, confirmação de origem, e anti-replay. A quantidade de serviços depende do SA estabelecido e do modo de operação.

O ESP tem o seguinte formato:



Os campos do ESP são:

- Security Parameters Index (SPI): É um valor de 32-bits do identificador único que inclui o protocolo (ESP) e endereço de destino, formando o identificador SA.
- Número de Seqüência: Este valor de 32-bits sem sinal contém um valor incremental do valor do número de seqüência (semelhante ao TCP). Isto faz a propriedade de anti-replay do ESP.
- Dados do Payload: Isto é um campo de tamanho variável que contém os dados referente ao pacote definido no Próximo Cabeçalho. Se um algoritmo de criptografia for usado, então os dados de sincronização também devem ser enviados (tais como Vetores de Inicialização). Se a sincronia for implícita, esta deve ser definida pela RFC.
- Padding (Enchimento): O enchimento pode ser usado porque um algoritmo de criptografia precisa de um múltiplo de certo tamanho, para definir delimitadores ou por enchimento para próprio cabeçalho ESP.
- Tamanho do Pad: Este campo indica que um número de bytes de enchimento está precedendo ele. O valor pode ser de 0 à 255.
- Próximo Cabeçalho: Um valor inteiro de 8 bits que identifica o que estará presente na parte de dados. É o mesmo valor definido pela IANA para os protocolos, exatamente igual ao IP e ao AH.
- Dados de Autenticação: Este campo variável contém um ICV calculado sobre o pacote ESP menos os dados do próprio campo de autenticação.

Igualmente ao AH, o ESP pode ser empregado em dois modos: transporte ou túnel. No modo transporte, o ESP é inserido após o IP e antes dos cabeçalhos superiores, provendo os serviços para os mesmos, tais como TCP, UDP, ICMP, etc.

Vejamos como fica isso:

IPv4

Pacote IP Original	TCP	Dados

IPv4

Pacote IP Original	ESP	TCP	Dados	ESP (Trailer)	Autenticação ESP
	← criptografado →				
← autenticado →					

No modo túnel, o ESP é usado em gateways de VPNs, e o gateway cria um novo cabeçalho IP para carregar o IP original.

IPv4

Novo Pacote IP	ESP	Pacote IP Original	TCP	Dados	ESP (Trailer)	Autenticação ESP
		← criptografado →				
	← autenticado →					

2.3.4 – Cabeçalhos AH e ESP simultaneamente

Como visto, o IPSec trabalha em dois modos: Transporte e Túnel. No modo transporte apenas o segmento da camada de transporte é autenticado e criptografado. No modo túnel, todo o pacote é autenticado e um novo datagrama é adicionado. O modo túnel é feito para uso em servidores VPN. O cabeçalho AH é inserido após o IP e antes do TCP/UDP/ICMP (ou ainda outro cabeçalho ESP), porém os endereços IPs originais ainda estão susceptíveis para alteração.

Porém além de aplicar AH ou ESP, o IPSec pode requerer suporte para combinações dos dois modos. A idéia é utilizar um túnel para autenticação e seu cabeçalhos internos (IP Original que aqui chamaremos de IP Original), e então aplicar AH ou ESP ou ambos externamente em modo de transporte para ampliar a proteção para o novo pacote e cabeçalho original criando um cabeçalho externo (Novo cabeçalho IP que aqui chamaremos IP Novo). Deve ser observado que em modo túnel, o AH e o ESP não são usados ao mesmo tempo, pois o ESP tem seu próprio esquema de autenticação. Isso é recomendado para pacotes quando o pacote interno (IP1) precisa autenticação e cifragem.

No modo Transporte o formato dos pacotes seriam:

IP Original	AH	Cabeçalhos Superiores

IP Original	ESP	Cabeçalhos Superiores

IP Original	ESP	AH	Cabeçalhos Superiores

No modo túnel o formato dos pacotes seriam:

Novo IP	AH	IP Original	Cabeçalhos Superiores

Novo IP	ESP	IP Original	Cabeçalhos Superiores

Porém existe um modo de fazermos ambos, chamado de modo combinado.

IP Novo	ESP	IP Novo	AH	IP Original	Cabeçalhos Superiores

IP Novo	AH	ESP	IP Novo	AH	IP Original	Cabeçalhos Superiores

Entretanto, nesta configuração não somente os pontos fortes do AH e ESP são combinados, mas também os problemas. Então você tem uma configuração que possui todos os problemas do NAT no AH e os pesos de processamento adicionais do ESP, somados ao processamento do AH. Essa relação provê uma segurança extra e um alto preço, e no mundo real, tais configurações são relativamente incomuns.

2.4 – IKE – Internet Key Exchange

O IKE (*Internet Key Exchange*) provê o gerenciamento da segurança para o *Security Association*. O IKE autentica cada ponto (host/gateways/servidores) de uma conexão IPSec, negocia políticas de segurança e manipula as trocas das chaves de sessão.

Além disso é possível usar certificados X509v3 para a autenticação dos equipamento envolvidos durante a negociação do IKE. O gerenciamento dos certificados inclui o uso do SCEP (Simple Certificate Enrollment Protocol), que permite a comunicação com uma Autoridade Certificadora (CA – Certificate Authority). Este certificado suporta ainda estrutura hierárquica para o uso em uma infra estrutura de chaves públicas (PKI – Public Key Infrastructure).

Os componentes para isso incluem o uso do protocolo de chaves públicas Diffie-Hellman para estabelecer uma chave de sessão mesmo estando em um meio inseguro, como a Internet.

Resumidamente o IKE provê quatro funcionalidades:

- Provê meios para as partes negociarem quais protocolos, algoritmos e chaves a serão usadas.
- Garante a identidade das partes, tanto do cliente, quanto do servidor.

- Gerencia as chaves após elas estarem em uso
- Garante que as trocas de mensagens que contém chaves sejam feitas por meios muito seguros.

Capítulo 3 - Algoritmos

O protocolo IPSec baseou-se em determinados padrões e algoritmos criptográficos para prover a confidencialidade, integridade e autenticação em níveis mais baixos, camada 3, camada de rede.

3.1 - Como funciona

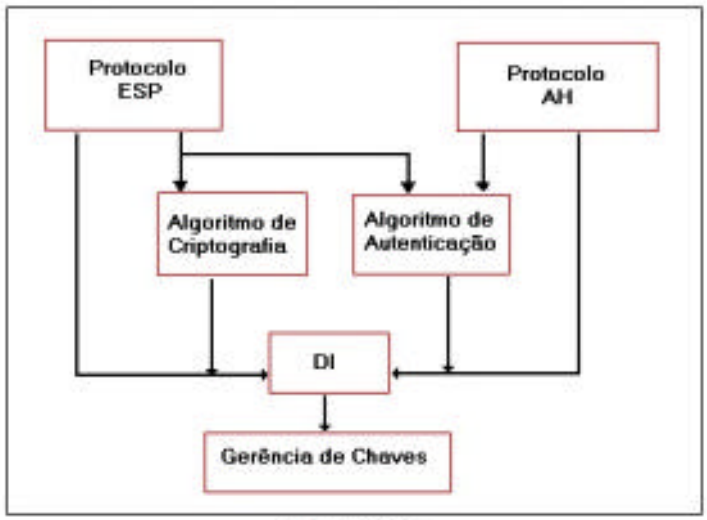
O uso dos algoritmos criptográficos na implementação do IPSec, baseai-se nos algoritmos já conhecidos como Diffie-Hellman, uso de chaves publicas entre outros. Abaixo seguem alguns protocolos:

- Protocolo Diffie-Hellman com a finalidade da troca de senhas secretas entre as partes de uma rede de dados pública;
- O uso de criptografia de chaves publicas para realizar a assinatura das trocas pelo Diffie-Hellman garantido a identidades das partes envolvidas no processo de comunicação;
- DES, 3DES e outros algoritmos para a criptografia dos dados;
- Algoritmos de resumo digital conhecidos como hash para a autenticação dos pacotes, como HMAC, MD5 e SHA-1;
- Certificados digitais para a validação de chaves públicas.

As tecnologias de criptografia foram traçadas nas RFCs 2406 e aprofundas nas RFCs 2408 e 2409.

3.2 - Quais os algoritmos envolvidos

Os componentes principais das tecnologias de criptografia são o cabeçalho de autenticação (AH – Aunthentication Header) e o protocolo de segurança (ESP – Encapsulation Security Payload) visto no capitulo anterior e estaremos aprofundando neste capitulo, e o gerenciamento de chaves que será abordado no capitulo seguinte de segurança. O projeto do AH e do ESP são modulares, o que possibilita o uso de novas implementações e algoritmos a medida que o mercado for evoluindo. Para realizar uma padronização o uso de uma determinada transação segura (**SA – Security Association**), o IPSec usa o conceito de Domínio de interpretação **(DI – Domain Interpretation),** no qual os algoritmos criptográficos, tamanho de chaves, formato, dentre outros são definidos primeiramente durante o estabelecimento da conexão segura. A figura abaixo ilustra o funcionamento:



Arquitetura do IPSec

Para cada fase da comunicação segura requer uma SA, sendo assim a mesma é necessária para a autenticação e para criptografia dos dados. Para isto mesmo que o algoritmo utilizado seja o mesmo o conjunto de chaves são distintas.

O cabeçalho de autenticação normalmente é colocado entre os campos IP e TCP e nenhuma modificação é realizada nos dados do pacote ou seja no payload. O cabeçalho AH, como visto anteriormete é composto de 5 campos contendo basicamente as informações do próximo cabeçalho, comprimento dos dados, índice dos paramêtros de segurança (SPI-Security Parameter Index), número de sequencia e dados de autenticação.

O SPI tem a função de informar ao receptor quais protocolos de segurança o remetente está utilizando para realizar a comunicação. Ou seja, para fazer autenticação dos dados ele está utilizando o HMAC (hash-based Message Authentication Code) aclopado com o MD5 (desenvolvido RSA) ou o SHA-1 (Secure Hash Algorithm Modified). Ultimamente o protocolo que vem sendo mais utilizado é o SHA devido as suas características de segurança é tido como mais imune aos ataques de colisão. Existe a combinação deste dois protocolos que é conhecida como HMAC-SHA-1, neste o hash tem 96 bits e é trucado após seu calculo. O AH possui também mecanismos para evitar retransmissões de pacotes o que causa os Denial of Services, são chamados de “anti-replay”.

O protocolo AH faz a autenticação somente do conteúdo do pacote o cabeçalho trafega em “clear text” pela rede, para realizar a confidencialidade dos dados faz se o uso de um outro protocolo, o ESP, já mencionado anteriormente. Este protocolo é responsável pela cifragem dos dados, ele é inserido entre o cabeçalho ip e o restante do datagrama. Juntamente com o ESP é inserido o SPI para informar como o pacote deve ser aberto. Um contador localizado no ESP informa quantas vezes um mesmo SPI foi direcionado a um determinado endereço IP de destino.Evitando ataques onde os pacotes são copiados e enviados fora de ordem.

Os algoritmos de criptografia mais utilizados são o DES e 3DES, a autenticação provida pelo ESP é diferente do AH pois ela não protege o cabeçalho IP que procede, embora o cabeçalho IP é protegido quando estiver em modo Túnel. O AH por sua vez

protege o cabeçalho externo, as duas soluções geralmente não são utilizadas em conjunto devido ao custo de processamento.

A finalidade dos protocolos AH e ESP é de garantir a segurança dos serviços envolvidos como: o controle de acesso, a integridade dos dados, a autenticação e confidencialidade dos mesmos. A figura abaixo mostra em quais protocolos estão presentes estas características:

Protocolo / Serviços	AH	ESP (simples)	ESP (combinado)
Controlo de acessos	**OK**	**OK**	**OK**
Integridade de pacotes	**OK**	**Não**	**OK**
Autenticação da origem	**OK**	**Não**	**OK**
IP Replying **Detecção e rejeição**	**OK**	**OK**	**OK**
Confidencialidade de Pacotes	**Não**	**OK**	**OK**
Confidencialidade em modo limitado	**Não**	**OK**	**OK**

Capítulo 4 - Segurança

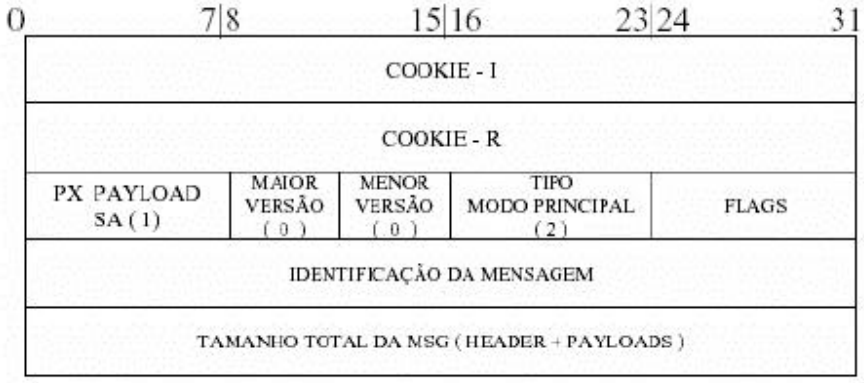
4.1 - Gerenciamento de Chaves

O gerenciamento de chaves realizado pelo IPSec pode ser realizado de forma manual ou automático dependo do numero de sites conectados. È um dos processos mais importantes do IPSec e da segurança que ele possui. Um dos ataques que pode ser evitado com o correto gerenciamento das chaves é o "man-in-the-middle" no qual um intruso pode capturar as trocas de informações entre a comunicação entre dois hosts.

O IKE está relacionado intimamente com o gerenciamento do SA. Quando um SA é criado, as chaves devem ser negociadas. IPSec também provê um meio para o uso de chaves manuais, gerenciados por um administrador de rede, porém em uma rede grande isso é muito difícil de ser feito.

Na realidade, o IKE é baseado em uma combinação de protocolos: o ISAKMP (Internet Security Association and Key Management Protocol) que é responsável pela negociação da segurança e o SKEME (Security Key Exchange Mechanism) responsável pela troca de chaves.

Segue a estrutura do cabeçalho do protocolo ISAKMP (o protocolo de transporte utilizado é o UDP, na porta 500):



- Cookie – valores aleatórios gerados pelas entidades. Utilizados contra ataques de replay e DoS. Também são utilizados para identificação da SA entre as duas entidades depois que a negociação for concluída;

- Px payload – responsável pela identificação do tipo do próximo payload do pacote. Este campo pode assumir os seguintes valores:

0 - Nenhum (último payload)
1 - Security Association
2- Proposta
3 - Transformação
4 - Troca de Chaves
5- Identificação
6- Certificado (CERT)
7 - Pedido de Certificado

8 - Hash
9 - Assinatura
10 - Nonce
11- Notificação
12 - Deleção
13 - ID de vendedor
Reservado **14 – 127**
Uso Particular **128 – 255**

- Versão - atualmente tem valor 1;
- **Tipo de comunicação** – responsável pela determinação das mensagens e dos payloads seguintes.
- **Flags** – indicam opções utilizadas na comunicação (RFC2408);
- **Identificação** – responsável em identificar unicamente uma mensagem. Utilizado durante a fase 2;
- **Tamanho** – tamanho total da mensagem (Header + Payload).

O protocolo IKE opera em duas fases:

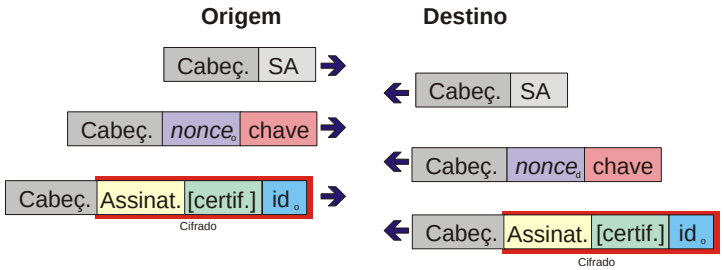
1º Fase: os dois pares estabelecem um canal seguro para realizar as operações do ISAKMP (ISAKMP SA);
2º Fase: os dois pares negociam os SA de propósito geral.
O objetivo de dividir em fases é de eliminar redundâncias entre os pontos de negociação do SA e consequentemente ganho de processamento, pois o canal seguro já está estabelecido na primeira fase.

O IKE pode estabelecer as chaves de três maneiras: Modo Normal, Agressivo ou Rápido (Main Mode, Aggressive mode and Quick Mode).

4.1.1 Modo Principal (Main mode)

Faz a fase de troca do ISAKMP, ou seja o estabelecimento do canal seguro de comunicação. È composto de 3 fases com 2 mensagens cada

- ***Fase1*:** as partes envolvidas trocam informações sobre os algoritmos e hashes basicos a serem utilizados.
- ***Fase2:*** trocam chaves publicas para uma negociação Diffie Helman e fornecem os números aleatórios que a outra parte deve de assinar e devolver para provar sua identidade.
- ***Fase3:*** é verificado as identidades. Quando o método de autenticação escolhido for o de Chave Compartilhada, a chave será derivada de um segredo, sendo utilizada uma função de hash nessa chave derivada que será trocada entre as duas entidades, sendo esta a informação de autenticação. Se o método de autenticação escolhido for o de Assinatura Digital, será necessário o uso de Certificado Digital que contenha a Assinatura das entidades a serem autenticadas;



nonce = Dados nonce (aleatório)
Cert. = Certificado Digital (opcional)
Assinat. = Assinatura do desafio remoto

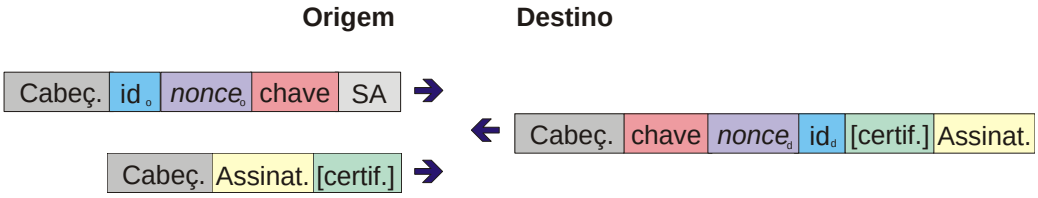
ID = Payload de Identificação
Chave = Payload de Chaves
Assinat. = Assinatura do desafio remoto

4.1.2 Modo Agressivo (Agressive mode)

É uma outra forma de realizar a troca do ISAKMP, atuando de forma mais simples e rápido do que o modo anterior, mas em compensação não protege as identidades dos membros envolvidos na negociação, porque ele transmite suas identidades antes do estabelecimento do canal seguro de comunicação.

No primeiro passo, onde passada a proposta de SA, a chave, o nonce para a outra entidade assinar, e um ID para verificar a identidade do emissor. No segundo passo o receptor responde com os dados necessário, finalizando com o emissor confirmando os dados no terceiro passo.

Como o Modo Agressivo tem apenas uma etapa, ele tem menor overhead, fazendo com que seja mais rápido do que o Modo Principal. Mas o modo mais utilizado e mais seguro é o Modo Principal, principalmente porque no Modo Agressivo as informações de autenticação não são criptografadas.



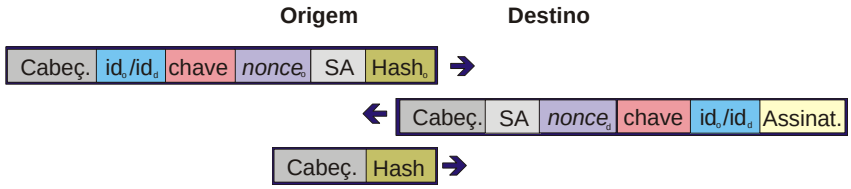
nonce = Dados nonce (aleatório)
Cert. = Certificado Digital (opcional)
Assinat. = Assinatura do desafio remoto

ID = Payload de Identificação
Chave = Payload de Chaves
Assinat. = Assinatura do desafio remoto

4.1.3 Modo Rápido (Quick mode)

Faz a segunda fase da troca ou seja realiza a negociação de um SA para a comunicação de uso geral. No passo 1 o emissor envia uma mensagem com hash, um nonce, os ID's identificando cada entidade, além dos parâmetros da proposta de SA. No passo 2 o receptor responde com uma mensagem parecida, acrescentando

seu próprio nonce e hash para confirmação. No passo 3 o emissor responde com um hash dos dois nonces, assim, completando a troca e estabelecendo o SA IPSec. Para evitar que um intruso que capturou a chave utilizada na fase 1 descriptografe a comunicação da fase 2, pode-se utilizar a técnica Perfect Forward Secrecy, onde a chave será derivada por meio do algoritmo de Diffe- Helman. Este procedimento reduz a performance, mas aumenta a segurança da comunicação.



nonce = Dados nonce (aleatório)
Cert. = Certificado Digital (opcional)
Assinat. = Assinatura do desafio remoto
ID = Payload de Identificação
Chave = Payload de Chaves
Assinat. = Assinatura do desafio remoto

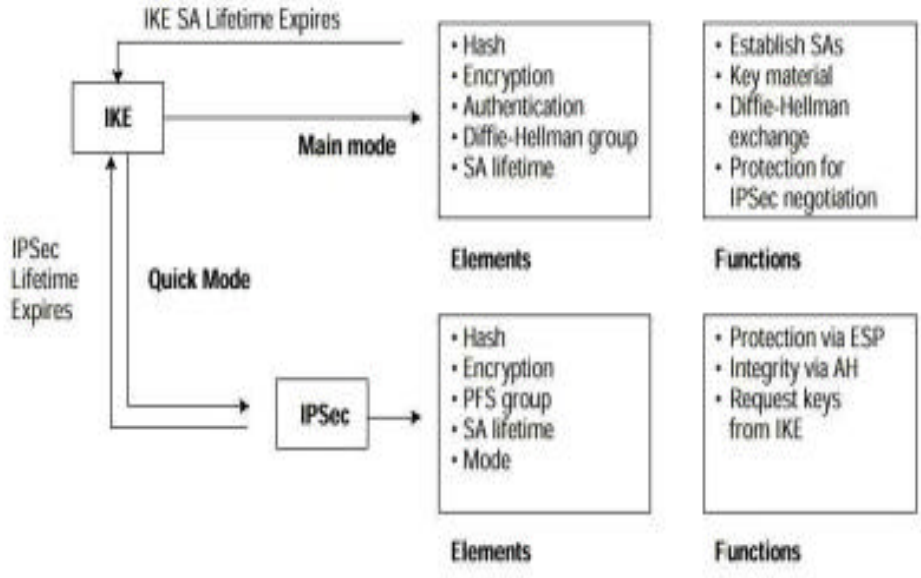
O IKE possui também um modo chamado de **Modo Novo (New Group mode)**, no qual provê a fase um de negociação e é utilizado para definir um mecanismo de grupos privados para a troca do tipo Diffie-Hellman.

Para o estabelecimento de uma conexão IKE segura, devemos seguir os itens abaixo:

- O algoritmo de criptografia para proteger dos dados;
- Um algoritmo de hash para assinatura digital;
- Um método de autenticação para assinar o hash;
- Informação sobre o qual grupo a troca Diffie-Hellman deve ser feita;
- Especificação da função pseudo randômica para fazer o hash de certos valores durante a troca de chaves, para a verificação. Se nada for especificado, o padrão é a versão HMAC.

Depois da negociação do SA, as entidades estão prontas para se comunicar em uma rede publica, de modo seguro, formando um túnel VPN.

Segue o diagrama com o fluxo das chaves de criptografia:



Um outro tipo de gerenciamento de chaves existente para o IPSec é **SKIP** (*Simple Key Managemment for IP*), utilizado pela San e Novell. Em vez de utilizar chaves orientadas a sessão, o Skip utiliza chaves orientadas a pacote, as quais são comunicadas em linha com os pacotes. Esse protocolo não faz parte do padrão em uso pelo grupo de trabalho do IPSec.

4.2 - Processamento do tráfego

Para o estabelecimento de uma conexão VPN com base em IPSec, existe alguns passos básicos: O gateway verifica através de uma política de segurança se o host pode ser conectado, ou seja criado um túnel virtual. Caso está verificação seja afirmativa o gateway inicia a negociação do Security Association (SA) da sessão; após isto o host se comunica por meio de um canal seguro.

Além de todos os itens de segurança aplicados a uma VPN como autenticidade da conexão e dos usuários, integridade. Um outro fator é muito importante é ao controle de trafego e qualidade de serviço e gerenciamento.

O controle do trafego faz se necessário para resolver uns dos problemas não só relacionado a VPNs para no trafego das redes em geral a qualidade de serviço. Este controle é realizado fundamentalmente pelo controle de banda, onde é determinado a largura que cada protocolo deve trafegar pela rede visando uma melhor desempenho das aplicações. Garantindo por exemplo uma banda para o IPSec pode evitar que o link de saida para a Internet esteja com alta utilização de trafego de HTTP e FTP e esteja impactando aplicações mais criticas que estejam em uma VPN. Existem outros protocolos que realizam a função de controle de banda dentre eles o MPLS e o DiffServ.

O gerenciamento tem como objetivo facilitar a integração da VPN com a política de segurança da organização por meio de gerenciamento local ou remoto. Existem ferramentas para auxiliar no processo de monitoração, solução de problemas e até

contabilidade do serviço. A contabilidade passa a ser importante para empresa que prove os serviço de VPN a terceiros, pois a cobrança pode ser realizada baseando-se na confiabilidade, alto desempenho ou níveis de serviços.

A garantia de qualidade de serviço pode ser incorporada aos níveis de custo, como por exemplo, pacotes que requer maior garantia de desempenho na rede podem ter uma valor diferenciado dos pacotes normais da rede. Antes de contratar estes tipos de serviços VPN, é interessante se atentar a algumas informações como: área de cobertura, acesso, desempenho, segurança, gerenciamento, largura de banda e garantia de qualidade de serviço.

4.3 - NAT com IPSec

Uma das utilizações mais comuns do IPSec está em fornecer as potencialidades para as VPNs que estão cada vez mais populares o uso das mesmas para a comunicação entre parceiros, entre empresas. Em paralelo a isto muitas delas utilizam o conceito de NAT (Network Address Translation) para realizar esta comunicação de forma mais segura e sem riscos de conflito de endereçamento entre as partes. Porem existe algumas restrições quanto ao uso do IPSec com o NAT que tornam uma das maiores barreiras de implantação de VPNs com IPSec. Iremos descrever estas incompatibilidades e como contorná-las.

As principais incompatibilidades entre NAT e IPSec podem ser divididas em três categorias:

5 **As intrínsecas do NAT:** Estas incompatibilidades derivam-se diretamente da funcionalidade do NAT descrita na RFC3022. Estas incompatibilidades estão presentes em qualquer equipamento com NAT.

6 **Fraquezas na implementação do NAT:** Estas incompatibilidades não são intrínsecas ao protocolo, porem estão presentes em muitas implementações como problemas em segurar fragmentos inbound ou outbound. Entretanto, se os problemas da implementação estiver espalhado pela rede é necessário fazer analises para uma solução traversal de NAT.

7 **Incompatibilidade "Helper":** Estas incompatibilidades estão presentes nos dispositivos de NAT que tentam fornecer para IPsec NAT traversal. De um forma irônica, esta funcionalidade do "ajudante" cria algumas incompatibilidades adicionais, fazendo um problema já difícil mais complicado de ser resolvido. Quando a funcionalidade traversal do "ajudante" de IPsec não estiver presente em toda a implementação de NATs, estas características estão tornam-se cada vez mais populares e necessitam também de ser analisadas de uma forma transversal.

Vamos analisar cada um destes tópicos de incompatibilidade.

4.3.1 – Incompatibilidades intrínsecas do NAT:

As incompatibilidades intrínsecas entre NAT e IPSec incluem:

a) **IPsec Autentication Header** definido na RFC2402 **e NAT**. O cabeçalho AH, como visto anteriormente, incorpora o IP de origem e endereços de destino durante o

processo de checagem de integridade das chaves. Os dispositivos NAT ou NAT reversos que fazem mudanças nos campos de endereço invalidando a verificação da integridade da mensagem. O cabeçalho do IPsec ESP não incorpora o IP de origem e os endereços de destino durante o processo de checagem de integridade das chaves, desta forma este problema não ocorre com o protocolo ESP.

b) **Incompatibilidade entre o checksums e o NAT**. Os checksums de controle do TCP e do UDP têm uma dependência com Ip de origem e nos endereços de destino através da inclusão do "pseudo-encabeçamento" no cálculo. Como resultado, as somas de controle são calculadas e verificadas no receptor, invalidado a passagem do NAT ou do NAT reverso. Em contra partida, o IPSec ESP passa tranqüilo com o NAT se os protocolos TCP/UDP não estão envolvidos, como em um Tunel Ipsec ou no IPSec/GRE, ou se as somas de controle não são calculadas (como é possível com o UDP IPv4). Como descritos na RFC793, o cálculo da soma de controle do TCP e a verificação são requeridos no IPv4. O cálculo e a verificação da soma de controle de UDP/TCP são requeridos em IPv6. SCTP definido nas RFCs 2960 3309 usa um algoritmo de CRC32C calculado somente no pacote de SCTP (cabeçalho + chunks), de modo que o cabeçalho IP não seja coberto. Em conseqüência, NATs não invalida o SCTP CRC, e o problema de incompatibilidade não existe. È importante lembrar que o tráfego de IPsec deve ser garantida a integridade protegida e autenticada usando o criptografia forte, as modificações no pacote podem ser detectadas antes de verificar UDP/TCP.

c) **Incompatibilidade entre IKE e NAT** entre identificadores de endereço de IKE e NAT. Onde os endereços do IP são usados como identificadores em IKE milímetro ou QM, a modificação do IP de origem ou dos endereços de destino por NATs ou por NATs reverso resultará em uma mau combinação entre os identificadores e os endereços no cabeçalho IP. As execuções de IKE são requeridas para rejeitar tais pacotes. Para evitar o uso de endereços IP como identificadores de IKE milímetro e de QM, os userIDs e FQDNs podem ser usados preferivelmente. Onde a autenticação do usuário é desejado, um tipo do ID de ID_USER_FQDN pode ser ultilizado ou onde o a autenticação desejada da máquina, um tipo do ID de ID_FQDN pode ser utilizado. Em um ou outro caso é necessário verificar que a identidade proposta combina com aquela incluída no certificado. Entretanto, quando o uso tipos da identidade de USER_FQDN ou de FQDN for possível dentro de IKE, há os cenários do uso (por exemplo entradas do SPD que descrevem subnets) que não podem ser realizados desta maneira.

d) **Incompatibilidade entre sobrepor entradas do SPD e NAT**. Onde os hosts atrás de um NAT negociam entradas sobrepondo do SPD com o mesmo destino em IKE QM, os pacotes podem ser emitidos com IPsec errado. Isto ocorre porque ao remetente, o IPsec SAs parece ser equivalente, a não ser que existem entre os mesmos endpoints e podem ser usados passar o mesmo tráfego.

e) **Incompatibilidade entre a seleção de IPsec SPI e NAT**. No IPsec o tráfego é cifrado ESP e assim fica transparente ao NAT, os elementos NAT e ao cabeçalho de IPsec para desmultiplexar o tráfego de entrada do IPsec. A combinação do endereço

IP de destino, do protocolo da segurança (AH/ESP) e do IPsec SPI é tipicamente utilizado para este propósito. Entretanto, desde que o trafego de entrada e saída do SPIs escolhido seja independentemente, não há nenhuma maneira para que o NAT determine que SPI de destino corresponde a somente pelo tráfego de saída. Sendo assim dois hosts atrás do NAT ao tentar trazer acima simultaneamente IPsec SAs para o mesmo destino, é possível que o NAT emite os pacotes de entrada de IPsec ao destino errado. Note que isto não é tipicamente uma incompatibilidade com o IPSec mas tipicamente a maneira com que é implementado. Em ambos os protocolos AH e ESP, o host receptor especifica a SPI para ser utilizada na SA. combinação do IP do destino, do SPI, e do protocolo da segurança (AH, ESP) identifica excepcionalmente uma associação da segurança. Isto significa que o host de recepção pode selecionar SPIs tais que tem uma associação da segurança (SA) como por exemplo: (SPI=470, Dest IP=10.2.3.4) e uma associação diferente da segurança com (SPI=470, Dest IP=10.3.4.5).

f) **Incompatibilidade entre endereços agregados aos Ips e NATs**. Desde que no payload a integridade é protegida, nenhum dos endereços IP incluídos dentro dos pacotes do IPSec serão transladados por um NAT. Isto gera uma ineficiência na ALGs (Application Layer Gateways) implementadas com o NAT. Protocolos que utilizam os endereços agregados ao Ip como o FTP, IRC, SNMP, LDAP, o H323, o SIPm o SCTP. Para corrigir este problema é necessário instalar as ALGs no host ou security gayeway que pode operar com o trafego da aplicação antes do encapsulamento IPSec e após o decapsulamento do IPSec.

g) **Implícito direcionamento para o NAT**: requer que o pacote de inicial de saída percorra fim a fim criando um traçado de inbound. Proíbe o estabelecimento de de conexões IPSec não solicitadas para hosts atras do NAT.

4.3.2 – Fraquezas na implementação do NAT:

Durante a implementação alguns problemas são citados:

a) **Inabilidade suportar o tráfego de non-UDP/TCP**. O tráfego de IPSec é descartado, ou seja é incapaz de passar tráfego: SCTP, ESP (protocolo 50) ou AH (protocolo 51).
b) **Mapeamento de timeouts.** Os NATs varia de tempo o com o mapeamento UDP e será mantido na ausência do trafego, nivelando assim onde os pacotes de IKE podem ser corretamente traduzidos, o estado de tradução pode ser removido prematuramente se o timeout expirar.
c) **Inabilidade de suportar fragmentação**: maioria dos NATs podem corretamente fragmentar pacotes IP se o tamanho do pacote do IP exceder o MTU. Entretanto, a tradução apropriada dos pacotes que são fragmentados já são difíceis e a maioria de NATs não seguram esta funcionalidade corretamente. Como por exemplo: onde

dois hosts originam pacotes fragmentados para o mesmo destino, os identificadores do fragmento podem se sobrepor. Desde que o host de destino confia no identificador na fragmentação para a remontagem, o resultado será corrupção de dados. Poucos NAT protegem às colisões do identificador suportando a tradução do mesmo. As colisões do identificador não são um problema do NATs quando executa a fragmentação se o identificador do fragmento necessitar somente de um único origem/destino por vez. Desde que somente o primeiro fragmento conterá tipicamente um cabeçalho completo de IP/UDP/SCTP/TCP, a necessidade de NATs poder executar a tradução baseado no identificador do endereço IP e do fragmento de origem/destino sozinho. Desde que os fragmentos podem ser requisitados novamente, os cabeçalhos a um identificador dado do fragmento não podem ser reconhecidos se um fragmento subseqüente chegar antes do inicial, e os cabeçalhos podem ser divididos entre os fragmentos. Em conseqüência, o NAT pode necessitar executar a remontagem antes de terminar a tradução. Poucas implementações de NAT fazem isto. Note que com NAT, o endereço IP de origem/destino são bastantes para determinar a tradução, no entanto, é possível para que os cabeçalhos de IPsec ou de IKE sejam divididos entre os fragmentos, de modo que na remontagem possa ainda ser requerida.

4.3.3 – Incompatibilidade “Helper”:

Segue algumas incompatibilidades entre o IPSec e a funcionalidade do NAT Helper:

a) **Inspeção do cabeçalho ISAKMP.** Atualmente algumas implementações de NAT utilizam cookies IKE para demultiplexar o tráfego de entrada do IKE. Como porta de origem, o cookie IKE multiplexado resulta em problemas com a redistribuição de chaves, desde a fase primeira fase de redistribuição tipicamente não usará os mesmos cookies que o tráfego mais adiantado.

b) **Tratamento especial da porta 500**. Em algumas implementações IKE não são capazes de garantir a porta de origem UDP 500. Alguns NATs não traduz pacotes com esta porta de origem UDP, isto significa que estes NATs são limitados para o client IPSec trocar informações com o gateway de destino, ao não ser que sejam inspecionados os detalhes do cabeçalho do ISAKMP para examinar os cookies que gera o problema acima.

c) **Inspenção do payload ISAKMP**. As implementações de NAT que analisam o payload ISAKMP podem não suportar todos os tipos de combinação de ordenação de payloads, ou suportar o payload de vendedor_ID para a opção de negociação do IKE.

4.4 – Requerimentos para compatibilidade

Para estabelecer uma solução de implementação de IPSec com NAT, além do estabelecimento de túneis IPSec, alguns itens devem ser levados em conta:

8 **Distribuição:** Embora as implementações de NATs com o Ipv6 sejam, relacionado a tempo, mais facilmente resolvidas ainda levará se um bom tempo para que o uso desta tecnologia amadureça no mercado uma vez que terá que haver a troca de routers e novas implementações em hosts enquanto que trabalhar com as incompatibilidades existentes na implementação de NAT com IpSec no Ipv4. Pois as incompatibilidades deve ser resolvidas em uma escala de tempo menor que a difusão do Ipv6.

9 **Compatibilidade de Protocolos:** uma solução transversal NAT de IPsec não se espera resolver edições com protocolos que não podem atravessar NAT com IPSec. Consequentemente, ALGs pode ainda necessitar de alguns protocolos, mesmo quando uma solução transversal NAT de IPsec está disponível.

10 **Segurança:** desde que o NAT direto tem a função de segurança, IPsec NAT e as soluções transversais não devem permitir a entrada do trafego IPsec de forma arbitraria. Sendo assim nenhum IP a ser recebido por um host atrás do NAT, embora mapeamento o estado deve ser mantido de forma bidirecional para que a conexão IKE e IPSec seja estabelecida.

11 **Cenário de Telecomutadores:** O cenário de telecomutadores desde do uso do IPSec para o acesso remoto a Intranets Corporativas, uma solução transversal de NAT DEVE suportar NAT transversal através da modalidade de túnel de IPsec ou do transporte de L2TP IPsec [RFC 3193]. Isto inclui suporte para transversal de mais de um NAT entre o cliente remoto e o Gateway VPN. O cliente pode ter um endereço roteável e o Gateway VPN pode estar atrás de um NAT, ou alternativamente, o cliente e a Gateway VPN podem ser atrás de um ou mais NATs. Telecomutadores pode usar o mesmo IP confidencial, cada um atrás de seu próprio NAT, ou muitos telecomutadores podem residir em uma rede confidencial atrás do mesmo NAT, cada uma com seu próprio endereço confidencial original, conectando à mesmo Gateway VPN. Desde que IKE utilize a porta 500 do UDP como o destino, não é necessário permitir gateways múltiplos de VPN que operam-se atrás do mesmo endereço IP externo. Em um cenário gateway-gateway uma rede privada (DMZ) pode ser introduzida entre a rede corporativa e a Internet. Neste projeto, conectar gateways segurança de Ipsec com endereços privados.

12 **Compatibilidade de Firewall:** Desde que os firewalls são desenvolvidos, a solução de compatibilidade de NAT-IPsec deve estar habilitada para o administrador criar, regras de acessos estáticos para permitir ou rejeitar o trafego transversal de IKE e IPSec NAT. Isto implica, para o exemplo, que o alocação de portas dinâmicas de IKE ou de IPsec deve ser evitado.

13 Escala: Uma solução IPsec-NAT da compatibilidade deve ser capaz de ser desenvolver a instalação de vários telecomutadores. Nesta situação, não é possível

supor que somente um único host estará comunicando com um destino em um dado momento. Assim, uma solução IPsec-NAT compatível deve atentar-se a sobreposição dos dados.

4.5 – Ataque aos Clientes de VPN

Quando um cliente VPN age como um roteador ou gateway, isto pode causar sérios problemas de segurança na rede. Isto acontece porque o cliente VPN possui duas conexões ativas (Internet e um acesso a VPN). Desta maneira, um hacker pode utilizar a conexão da Internet para ter acesso para a conexão da VPN, e assim o hacker pode injetar dados "autenticados e cifrados" para o ataque na matriz.
Uma maneira de evitar esses problemas é remover o recurso de roteamento de pacotes neste cliente. Por padrão clientes não devem rotear pacotes para a rede interna da organização, ou que essas sejam usadas só em último caso.
Uma outra possibilidade de forçar o roteamento é a utilização de source-routing, que se aceito pela máquina poderia fazer uma rota que seria impossível, ou ainda usar este ataque para criar rotas de retorno para ataques do tipo "IP Spoofing"
Sem contar que o cliente VPN pode ser atacado através de falhas nas aplicações (tais como ataques de Buffer Overflow), fazendo com que esta esteja sob domínio do hacker. Se isso acontecer, o hacker terá pleno acesso à rede corporativa da empresa através da VPN, ou ainda abusar da relação de confiança da matriz com os clientes VPNs autenticados. [PLG03]

Capítulo 5 – Implementações IPSec

5.1 - Windows 2000/2003

O Microsoft Windows 2000 Server inclui uma implementação da Internet Protocol Security (IPSec, segurança do protocolo da Internet), baseada nos padrões IETF para IPSec. A implementação da segurança IP no Windows 2000 foi criada para proteger as comunicações ponta-a-ponta entre hosts. Supõe-se que o que está entre eles, o meio usado para a transmissão de dados, não é seguro.

Os dados do aplicativo do host que está iniciando a comunicação são criptografados de forma transparente antes de serem enviados através da rede. No host de destino, os dados são descriptografados de forma transparente antes de serem passados para o aplicativo receptor. Criptografar todo o tráfego da rede IP garante que qualquer comunicação que use o TCP/IP esteja protegida contra escutas. Como os dados são transmitidos e criptografados no nível do protocolo IP, não são necessários pacotes de segurança distintos para cada protocolo do stack TCP/IP.

Geralmente, um nível alto de segurança aumenta a administração. O Windows 2000 fornece uma interface administrativa, o IP Security Policy Management, para gerenciar de forma centralizada as diretivas, equilibrando facilidade de uso e segurança. As diretivas de IPSec podem ser facilmente configuradas para atender às exigências de segurança de um usuário, grupo, aplicativo, domínio, site ou empresa global. As diretivas se baseiam em metodologias críticas de filtragem de IP, deixando que você permita ou bloqueie as comunicações em um nível alto (sub-redes inteiras) ou em um nível granular (protocolos específicos em portas específicas), conforme julgado necessário.

O IPSec pode fornecer um nível alto de proteção devido à sua implementação no nível de transporte IP (camada 3 da rede). A segurança da camada 3 fornece proteção para todos os protocolos de camadas superiores e IP do conjunto de protocolos TCP/IP (TCP, UDP, ICMP, Raw [protocolo 255] e até mesmo protocolos personalizados). Aplicativos que usam TCP/IP transmitem os dados para a camada do protocolo IP, onde os dados são protegidos pela IPSec.

Os mecanismos de segurança que funcionam acima da camada 3, por exemplo o Secure Sockets Layer (SSL, camada de soquetes de seguros), só protegem aplicativos que usam o SSL, como navegadores da Web. Os mecanismos de segurança que funcionam abaixo da camada 3, por exemplo criptografia da camada de link, não são portáveis para comunicação pela Internet ou intranet encaminhada.

Ao funcionar na camada 3, a IPSec é transparente para usuários e aplicativos. Você não precisa de pacotes de segurança distintos para cada protocolo do conjunto TCP/IP. Assim que as diretivas estiverem configuradas, os usuários não vão precisar agir para proteger os dados.

5.1.1 - Diretivas da segurança IP

O recurso IPSec é implantado através das diretivas do Windows 2000. Diversas diretivas de segurança podem existir para um determinado domínio, mas os componentes das diretivas são constantes.

Diretivas de negociação: As diretivas de negociação determinam os serviços de segurança usados durante uma comunicação. Você pode escolher entre serviços que incluem confidencialidade (ESP) ou que não fornecem confidencialidade (AH), ou o algoritmo de segurança IP pode ser especificado. Também é possível se definir diversos métodos de segurança para cada diretiva de negociação. Se o primeiro método não for aceito para a associação de segurança, o serviço ISAKMP/Oakley vai prosseguir na lista até encontrar um método que possa ser usado para estabelecer a associação.

Diretivas de segurança: Cada configuração dos atributos da segurança IP é chamada de diretiva de segurança. As diretivas de segurança são compostas de diretivas de negociação e filtros IP associados. As diretivas de segurança são associadas às diretivas do controlador de domínio. Uma diretiva de segurança IP pode ser atribuída às Diretivas de domíno padrão, Diretivas locais padrão ou diretivas de domínio personalizadas criadas por você. Um computador que efetua logon no domínio vai aproveitar automaticamente as propriedades das diretivas de domínio padrão e locais padrão, incluindo as diretivas de segurança IP atribuídas a essas diretivas de domínio.

Filtros IP: Os filtros IP determinam ações diferentes a serem tomadas com base no local de destino de um pacote de IP, no protocolo IP que está sendo usado (por exemplo, TCP ou UDP) e nas portas relacionadas que são usadas pelo protocolo. O próprio filtro é usado como um padrão para correspondência de pacotes IP. Cada pacote IP é verificado em relação ao filtro IP e, se houver uma correspondência, as propriedades das diretivas de segurança associadas são usadas para enviar a comunicação.

5.1.2 - Opções de segurança IP

Parte das diretivas de negociação de IPSec determina a função a ser desempenhada por um computador durante a comunicação. Três modos básicos de funcionamento podem ser atribuídos a um computador:

- **Respondedor:** Um respondedor vai se comunicar através de IPSec, quando solicitado. Isso pode resultar do fato de um respondedor iniciar uma sessão de comunicação com um computador que esteja funcionando no modo de iniciador ou de bloqueio ou de ser solicitado por um iniciador.
- **Iniciador:** Como padrão, um iniciador vai se comunicar através de IPSec. Se o computador de destino não oferecer suporte a comunicações seguras, um iniciador vai responder e se comunicar sem proteção.
- **Bloqueio:** Um computador no modo de bloqueio só vai se comunicar através de IPSec.

As diretivas básicas podem ser aprimoradas com filtros para fornecer aplicação granular das diretivas. Por exemplo, os computadores de um determinado departamento

podem ter diversas diretivas de negociação dependendo do endereço IP do computador com o qual está estabelecendo uma comunicação.

Os usuários experientes podem decidir que algoritmo HMAC será usado para garantir a integridade. HMAC-MD5 e HMAC-SHA fornecem o mesmo nível de proteção, com a diferença sendo o tamanho da chave usada para proteger as informações: MD5 usa uma chave de 128 bits e SHA, uma chave de 160 bits. Chaves mais compridas oferecem mais segurança.

Os usuários experientes também podem decidir que algoritmo será usado em serviços de confidencialidade. A confidencialidade é garantida usando-se o Digital Encryption Standard (DES, padrão de criptografia digital). 40DES é oferecido para garantir a compatibilidade com normas de exportação, que limitam o tamanho das chaves. 3DES, também chamado de DES triplo, oferece o tamanho padrão de chave de 56 bits ao passar três vezes pelo processo de criptografia. Em cada passagem, ele usa uma nova chave exclusiva, gerando a criptografia tripla das informações. Cipher Block Chaining (CBC, encadeamento de bloco cifrado) com DES (DES-CBC) também fornece um tamanho de chave de 56 bits e evita reprodução adicional.

5.1.3 - Planejando as diretivas de PKI e IPSec

O gerenciamento e a administração de IPSec estão integrados à interface de gerenciamento base do Active Directory.

Nos domínios do Windows 2000, a autenticação pode ser obtida através do protocolo Kerberos predefinido. Portanto, as infra-estruturas dos certificados não precisam ser implantadas para proteger clientes, servidores de arquivos ou UOs de segurança (um grupo de computadores em uma unidade organizacional [UO] do Active Directory com a finalidade de segurança).

Em situações de acesso remoto/VPN/roteador a roteador, os certificados de chave pública devem ser usados para autenticação (ou chaves pré-compartilhadas, no caso de roteador a roteador).

Em geral, as comunicações pela Intranet requerem níveis inferiores de segurança do que as comunicações de rede pública: sem confidencialidade; sem encapsulamento; permissão de comunicações não seguras. Isso vai acelerar a taxa de transferência das comunicações, permitindo ainda algum nível de segurança: integridade e autenticação.

As comunicações IPSec podem ser acionadas, aceitas ou impostas entre qualquer conjunto de computadores ou individualmente. Se os dados forem muito confidenciais, é fácil forçar um computador a aceitar somente comunicações de IPSec.

Em geral, já que o encapsulamento é adequado a níveis altos de segurança, as regras de IPSec que especificam o encapsulamento também devem ter um alto nível de segurança nas diretivas de negociação. Os dados vão estar trafegando, na verdade, em uma rede pública e, portanto, a confidencialidade (ESP) é em geral garantida. Como os pacotes são encapsulados, o que protege o cabeçalho inicial, não é necessário se associar ESP a AH para obter proteção de endereçamento (cabeçalho).

5.1.4 - Definindo níveis de segurança

A implementação de IPSec requer um equilíbrio entre tornar as informações facilmente disponíveis para o maior número de usuários e proteger informações críticas contra modificação e interpretação não autorizadas. As estruturas de segurança IP e do Windows 2000 devem ser analisadas durante o planejamento:

- Avalie os níveis de risco para determinar o nível adequado de segurança necessário.
- Determine as informações que devem ser criptografadas e o que deve ser protegido contra modificação.
- Defina diretivas de acordo com critérios de risco e proteja as informações categorizadas.

As considerações sobre diretivas também são influenciadas pela função dos computadores aos quais elas se aplicam: será usada uma segurança diferente para controladores de domínio, servidores da Web, servidores de acesso remoto, servidores de arquivos, servidores de bancos de dados, clientes da intranet e clientes remotos. A IPSec pode se tornar ineficiente rapidamente se não houver o planejamento e avaliação cuidadosos das diretrizes de segurança e o design e atribuição adequados das diretivas.

Antes de criar as diretivas de IPSec, você deve definir:

- o que deve ser protegido
- como protegê-lo
- onde protegê-lo
- quem vai gerenciar as diretivas
- se as exigências de exportação são uma questão a ser considerada

Os níveis de segurança a seguir são recomendados como diretrizes na implementação da estrutura geral de segurança do Windows 2000. Para maior clareza, os níveis de segurança de IPSec corresponderão a essa lista.

- Segurança mínima
- Segurança padrão
- Segurança alta

Níveis mínimos de segurança: Como padrão, a IPSec não é ativada. Se o plano de segurança não exigir nenhuma proteção em determinadas situações, nenhuma ação administrativa é necessária.

Níveis padrão de segurança: Não há uma definição exata dos níveis padrão de segurança. Eles podem variar bastante, dependendo das diretivas e da infra-estrutura da organização. A IPSec vai tentar atender a essa exigência ambígua com:

  - Diretivas e regras padrão
  - Serviços de confidencialidade são fornecidos como uma opção e, portanto, os serviços de proteção estão automaticamente em um nível padrão.

- Como padrão, as configurações ISAKMP, algoritmos de autenticação e de integridade, encapsulamento e nova geração de chaves são definidas no nível padrão.

Em geral, as comunicações pela intranet exigem níveis mais baixos de segurança do que as comunicações pela Internet, WAN ou redes externas: sem confidencialidade; sem encapsulamento; permissão de comunicações não seguras. Isso vai acelerar a taxa de transferência das comunicações pela intranet, permitindo ainda algum nível de segurança: integridade e autenticação.

Níveis altos de segurança: Um nível alto é adequado para situações dial-up remotas, comunicações WAN ou qualquer comunicação entre redes externas. As comunicações de redes particulares não devem ser excluídas automaticamente; em alguns casos uma segurança alta pode ser garantida para a intranet.

Novamente, não há uma definição exata pelos mesmos motivos, e a IPSec atende a esses critérios com:

- Serviços de confidencialidade para criptografar dados
- Sigilo perfeito de roteamento, duração configurável das chaves, limites Quick Mode, grupos Diffie-Hellman configuráveis e algoritmos extremamente resistentes (3DES e SHA).
- Encapsulamento para qualquer tipo de conexão de rede.
- A capacidade de associar ESP a AH para fornecer o nível mais alto de proteção: integridade de pacote e privacidade de dados.

Lembre-se de que nem todos os ataques vêm de fora das redes corporativas. Se for exigida uma segurança extremamente alta para uma intranet, encapsulamento deve ser usado, além das diretivas de negociação de alta segurança.

Quando os dados são extremamente confidenciais, não deve ser ativada a comunicação não protegida com um host que não reconhece IPSec, mesmo que o host esteja na mesma rede, pois isso não garante que os dados estejam protegidos.

Em geral, como o encapsulamento é adequado a níveis altos de segurança, as regras de IPSec que especificam o encapsulamento também devem ter um alto nível de segurança nas diretivas de negociação. Os dados estarão trafegando, na verdade, pela Internet e, portanto, os serviços de confidencialidade (ESP) estão geralmente garantidos.

5.2 - FreeBSD

Claramente esta estratégia permite que duas estações FreeBSD estabeleçam contato entre si - utilizando a VPN - porém é um meio muito ***famoso*** por ser utilizado para a conexão entre servidores.

É um método padrão, que pode ser utilizado inclusive entre servidores em outras plataformas.

A implementação de VPNs no FreeBSD é realizada utilizando-se do IPSec (ip Security Tunnel Mode) desenvolvido pela IETF. O IPSec é um protocolo padrão de camada 3 que oferece transferência segura de informações através de rede IP puplica ou privada. Uma conexão via IPSec envolve sempre 3 etapas:

1. Negociação do nível de segurança.
2. Autenticação e Integridade.
3. Confidencialidade.

Para implementar essas 3 etapas o IPSec utiliza-se de 3 mecanismos:

- AH - Autentication Header
- ESP - Encapsulation Security Payload
- ISAKMP - Internet Security Association and Key Management Protocol

No FreeBSD o IPSec suportado nativamente no kernel fornece os mecanismos de AH e ESP, já o serviço de ISAKMP é provido pelo aplicativo /usr/ports/security/racoon.

5.2.1 - Adicionando suporte ao IPSec ao seu kernel

Antes de iniciar a implantação da sua VPN é necessário incluir o suporte ao IPSec ao seu Kernel, para isso basta inserir as linhas abaixo no seu arquivo de configuração e recompilar o kernel:

```
options         IPSEC                   #IP security
options         IPSEC_ESP               #IP security (crypto; define w/ IPSEC)
options         IPSEC_DEBUG             #debug for IP security
pseudo-device   gif     4               #IPv6 and IPv4 tunneling
```

5.2.2 - Instalar o suporte a ISAKMP

Antes de instalar o racoon é recomendado que você sincronize a sua árvore do ports usando o cvsup para garantir que você estará instalando a ultima versão disponível.

Após sincronizar a sua arvore do ports, execute o comando abaixo:

```
# cd /usr/ports/security/racoon
# make clean
# make
# make install
```

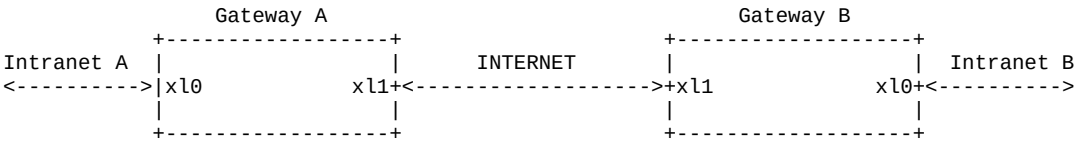
5.4.3 - Configuração do Firewall

Apesar de não ser obrigatório, é altamente recomendado que os seus gateways da VPN, rodem algum tipo de firewall, limitando a comunicação da interface publica do primeiro host apenas para a interface publica do segundo. Você pode usar o ipfw ou o ipfilter, fica a seu critério escolher aquele que você domina melhor.

Se você não definir uma boa política de segurança para os seus gateways, você pode colocar a segurança de sua VPN em risco, assim perca alguns minutos configurando seu firewall antes de começar a configurar uma VPN!!!

5.4.4 - Configuração

Antes de iniciar a configuração vamos considerar a seguinte estrutura:



Gateway A:

xl0 -> 192.168.1.1/255.255.255.0

xl1 -> 200.230.245.20/255.255.255.0

Gateway B:

xl0 -> 192.168.2.1/255.255.255.0

xl1 -> 200.220.125.50/255.255.255.0

Cada um dos hosts acima possui duas interfaces de rede, uma com ip publico e uma com ip invalido e ambos os hosts estão configurados para atuar como gateway.

5.4.4.1 - Como configurar sua VPN sem usar ISAKMP (chaves estáticas)

No Gateway A

Você deve criar o arquivo ***/usr/local/etc/rc.d/vpn.sh*** com o seguinte conteúdo:

```
#!/bin/sh
gifconfig gif0 200.230.245.20 200.220.125.50
ifconfig gif0 192.168.1.1 192.168.2.1 netmask 0xffffffff
route add -net 192.168.2.0/24 192.168.2.1
setkey -f /etc/ipsec.conf
Sete o arquivo criado acima como executável dando um chmod 755
/usr/local/etc/rc.d/vpn.sh.
```

Agora você precisa criar o arquivo ***/etc/ipsec.conf*** com o seguinte conteúdo:

```
flush;
spdflush;

add 200.230.245.20 200.220.125.50 esp 9991 -E blowfish-cbc
"Escolha_uma_Chave_para_a_conexao_A_B_quanto_maior_melhor";
add 200.220.125.50 200.230.245.20 esp 9992 -E blowfish-cbc
"Escolha_uma_Chave_para_a_conexao_B_A_quanto_maior_melhor";

spdadd 192.168.1.0/24 192.168.2.0/24 any -P out ipsec
```

```
esp/tunnel/200.230.245.20-200.220.125.50/require;
spdadd 192.168.2.0/24 192.168.1.0/24 any -P in ipsec
esp/tunnel/200.220.125.50-200.230.245.20/require;
```

No Gateway B

Você deve criar o arquivo ***/usr/local/etc/rc.d/vpn.sh*** com o seguinte conteúdo:

```
#!/bin/sh
gifconfig gif0 200.220.125.50 200.230.245.20
ifconfig gif0 192.168.2.1 192.168.1.1 netmask 0xffffffff
route add -net 192.168.1.0/24 192.168.1.1
setkey -f /etc/ipsec.conf
```

Sete o arquivo criado acima como executável dando um chmod 755 /usr/local/etc/rc.d/vpn.sh.

Agora você precisa criar o arquivo ***/etc/ipsec.conf*** com o seguinte conteúdo:

```
flush;
spdflush;

add 200.230.245.20 200.220.125.50 esp 9991 -E blowfish-cbc
"Escolha_uma_Chave_para_a_conexao_A_B_quanto_maior_melhor";
add 200.220.125.50 200.230.245.20 esp 9992 -E blowfish-cbc
"Escolha_uma_Chave_para_a_conexao_B_A_quanto_maior_melhor";

spdadd 192.168.2.0/24 192.168.1.0/24 any -P out ipsec
esp/tunnel/200.220.125.50-200.230.245.20/require;
spdadd 192.168.1.0/24 192.168.2.0/24 any -P in ipsec
esp/tunnel/200.230.245.20-200.220.125.50/require;
```

Obs: As chaves utilizadas no host A devem ser idênticas ao do Host B ou não vai funcionar!!!

Para subir sua VPN basta executar manualmente os arquivos ***/usr/local/etc/rc.d/vpn.sh*** em cada um dos hosts, se tudo esta funcionando como devia você já deve ser capaz de pingar os hosts de uma intranet para a outra, se tiver duvidas se o trafego esta realmente criptografado utilize o tcp dump para capturar alguns pacotes e o tráfego dos pacotes para certificar-se que tudo está funcionando.

A configuração acima já lhe proporciona um canal seguro de uma intranet para a outra, porem como estamos usando chaves estáticas essa configuração ainda não é a ideal, o próximo passo é configurar o uso de chaves dinâmicas. Nesta configuração uma chave predefinida é utilizada para iniciar a comunicação dos 2 hosts e em seguida uma nova chave aleatória é utilizada e alterada de tempos em tempos.

5.4.4.2. Como configurar sua VPN usando ISAKMP (chaves dinâmicas)

No Gateway A

Você deve criar o arquivo */usr/local/etc/rc.d/vpn.sh* com o seguinte conteúdo:

```
#!/bin/sh
gifconfig gif0 200.230.245.20 200.220.125.50
ifconfig gif0 192.168.1.1 192.168.2.1 netmask 0xffffffff
route add -net 192.168.2.0/24 192.168.2.1
setkey -f /etc/ipsec.conf
/usr/local/sbin/raccoon
```

Sete o arquivo criado acima como executável dando um chmod 755 /usr/local/etc/rc.d/vpn.sh.

Agora crie o arquivo */usr/local/etc/racoon/chave.txt* com o seguinte conteúdo:

```
200.220.125.50 Escolha_uma_Chave_para_a_conexao_A_B_quanto_maior_melhor
```

O próximo passo é criar o arquivo de configuração do racoon, crie o arquivo */usr/local/etc/racoon/racoon.conf* com o seguinte conteúdo:

```
path pre_shared_key "/usr/local/etc/racoon/chave.txt" ;
log info;

remote anonymous
{
        exchange_mode aggressive,main;
        doi ipsec_doi;
        situation identity_only;

        nonce_size 16;
        lifetime time 2 hour;   # sec,min,hour
        lifetime byte 50 MB;    # B,KB,GB
        initial_contact on;
        support_mip6 on;
        proposal_check obey;    # obey, strict or claim

        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key ;
                dh_group 2 ;
        }
}

sainfo anonymous
{
        pfs_group 2;
        lifetime time 1 hour;
        lifetime byte 50000 KB;
        encryption_algorithm 3des,des,cast128,blowfish;
        authentication_algorithm hmac_sha1,hmac_md5;
        compression_algorithm deflate ;
}
```

Agora você precisa criar o arquivo */etc/ipsec.conf* com o seguinte conteúdo:

```
flush;
spdflush;

spdadd 192.168.1.0/24 192.168.2.0/24 any -P out ipsec
esp/tunnel/200.230.245.20-200.220.125.50/require;
spdadd 192.168.2.0/24 192.168.1.0/24 any -P in ipsec
esp/tunnel/200.220.125.50-200.230.245.20/require;
```

No Gateway B

Você deve criar o arquivo */usr/local/etc/rc.d/vpn.sh* com o seguinte conteúdo:

```
#!/bin/sh
gifconfig gif0 200.220.125.50 200.230.245.20
ifconfig gif0 192.168.2.1 192.168.1.1 netmask 0xffffffff
route add -net 192.168.1.0/24 192.168.1.1
setkey -f /etc/ipsec.conf
/usr/local/sbin/raccoon
```

Sete o arquivo criado acima como executável dando um chmod 755 /usr/local/etc/rc.d/vpn.sh.

Agora crie o arquivo */usr/local/etc/racoon/chave.txt* com o seguinte conteúdo:

```
200.230.245.20 Escolha_uma_Chave_para_a_conexao_A_B_quanto_maior_melhor
```

O próximo passo é criar o arquivo de configuração do racoon, crie o arquivo */usr/local/etc/racoon/racoon.conf* com o seguinte conteúdo:

```
path pre_shared_key "/usr/local/etc/racoon/chave.txt" ;
log info;

remote anonymous
{
        exchange_mode aggressive,main;
        doi ipsec_doi;
        situation identity_only;

        nonce_size 16;
        lifetime time 2 hour;   # sec,min,hour
        lifetime byte 50 MB;    # B,KB,GB
        initial_contact on;
        support_mip6 on;
        proposal_check obey;    # obey, strict or claim

        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key ;
                dh_group 2 ;
        }
}
```

```
sainfo anonymous
{
        pfs_group 2;
        lifetime time 1 hour;
        lifetime byte 50000 KB;
        encryption_algorithm 3des,des,cast128,blowfish;
        authentication_algorithm hmac_sha1,hmac_md5;
        compression_algorithm deflate ;
}
```

Agora você precisa criar o arquivo */etc/ipsec.conf* com o seguinte conteúdo:

```
flush;
spdflush;

spdadd 192.168.2.0/24 192.168.1.0/24 any -P out ipsec
esp/tunnel/200.220.125.50-200.230.245.20/require;
spdadd 192.168.1.0/24 192.168.2.0/24 any -P in ipsec
esp/tunnel/200.230.245.20-200.220.125.50/require;
```

Novamente, para iniciar sua VPN basta executar o arquivo /usr/local/etc/rc.d/vpn.sh em cada um dos gateways. Após inicializar a VPN verifique o arquivo de log /var/log/racoon.log para ver se esta tudo OK, caso não funcione verifique com um setkey -D se o suporte ao IPSec esta habilitado no seu kernel.

As configurações propostas neste tutorial para o racoon são básicas e são o mínimo necessário para que você inicie uma VPN com chaves dinâmicas, mas existem muitas outras opções, por ex: o uso de uma chave RSA para a fase inicial de autenticação, etc.

5.3 - FreeSWAN (Linux)

O FreeSWAN é a implementação mais famosa do Linux para o IPSec. O FreeSWAN possui suporte aos três protocolos do IPSec: AH, ESP e IKE.

O IPSec consegue controlar todos os protocolos baseados em IP, ao invés dos específicos, tais como SSL para HTTP, PGP para e-mail, SSH para Login Remoto, etc.

A implementação do FreeSWAN é dividida em 3 partes:

KLIPS (Kernel IPSec) que implementa o AH e ISP, além de prover a manipulação dos pacotes no kernel

Pluto (IKE) que implementa o IKE, negociando e mantendo conexões com outros sistemas

Scripts Proprietários para administração das conexões (interfaces)

Além disso o FreeSWAN possui uma boa compatibilidade com outros sistemas de VPN, desde Windows 2000, Checkpoint VPN-1, SSH Sentinel, etc.

Um item que deve se ter atenção é que a maioria dos recursos pode ser feita automaticamente, porém a identificação e autenticação dos gateways não podem ser realizadas automaticamente. Para isso, ou se cria um método onde as chaves são manuais, onde os administradores colocarão as chaves dentro dos arquivos de configuração, ou automaticamente, que é mais segura, mas a autenticação automática requer que exista um segredo (tal como uma senha) para confiança ou o uso de certificados de segurança.

5.3.1 - Como Instalar?

Primeiramente, se a sua distribuição de Linux já inclui uma distribuição do FreeSWAN, você deverá gerar uma nova chave, para evitar o uso de uma chave que esteja compilada junto com a distribuição.

Para isso, logado como root, deve-se executar.

```
    ipsec newhostkey --output /etc/ipsec.secrets --hostname
xy.example.com
    chmod 600 /etc/ipsec.secrets
```

Nota: Você deve substituir xy.example.com com o FQDN (Fully Qualified Domain Name) do seu servidor.

O resultado do arquivo ipsec.secrets vai ser:

```
: RSA   {
        # RSA 2192 bits   xy.example.com   Sun Jun 8 13:42:19 2003
        # for signatures only, UNSAFE FOR ENCRYPTION
        #pubkey=0sAQOFppfeE3cC7wqJi...
        Modulus: 0x85a697de137702ef0...
        # everything after this point is secret
        PrivateExponent: 0x16466ea5033e807...
        Prime1: 0xdfb5003c8947b7cc88759065...
        Prime2: 0x98f199b9149fde11ec956c814...
        Exponent1: 0x9523557db0da7a885af90aee...
        Exponent2: 0x65f6667b63153eb69db8f300dbb...
        Coefficient: 0x90ad00415d3ca17bebff123413fc518...
        }
# do not change the indenting of that "}"
```

Se sua distribuição, não possui o FreeSWAN, então você deve baixá-lo. Cada Kernel possui uma distribuição levemente diferente, para isso você deverá obter usando um script

```
(para Kernel 2.6)
ncftpget ftp://ftp.xs4all.nl/pub/crypto/freeswan/binaries/RedHat-
RPMs/\*userland*

(para kernel 2.4)
ncftpget ftp://ftp.xs4all.nl/pub/crypto/freeswan/binaries/RedHat-
RPMs/`uname -r | tr -d 'a-wy-z'`/\*
```

que será traduzido para
ncftpget ftp://ftp.xs4all.nl/pub/crypto/freeswan/binaries/RedHat-RPMs/2.4.20-9/freeswan-userland-2.04_2.4.20_9-0.i386.rpm

Em uma aplicação verdadeira, você deverá verificar hashs MD5 e assinaturas PGP do arquivo a ser instalado.

Para instalar, apenas use:

```
rpm –ivh freeswan*.rpm
```

Para iniciar o FreeSWAN basta usar:

```
service ipsec start
```

E para verificar a instalação você pode usar:

```
ipsec verify
```

```
Checking your system to see if IPsec got installed and started correctly
Version check and ipsec on-path                                 [OK]
Checking for KLIPS support in kernel                            [OK]
Checking for RSA private key (/etc/ipsec.secrets)               [OK]
Checking that pluto is running                                  [OK]
```

Lembre-se de liberar os pacotes para UDP porta 500, protocolos ESP e AH (50 e 51). Também recomenda-se remover eventuais NAT aos pacotes a serem tunelados.

Um exemplo em iptables poderia ser:

```
# IKE negotiations
iptables -I INPUT  -p udp --sport 500 --dport 500 -j ACCEPT
iptables -I OUTPUT -p udp --sport 500 --dport 500 -j ACCEPT
# ESP encryption and authentication
iptables -I INPUT  -p 50 -j ACCEPT
iptables -I OUTPUT -p 50 -j ACCEPT
```

5.3.2 - Um exemplo de uma conexão Site-to-Site

Para uma conexão site-to-site, algumas informações devem estar disponíveis, tais como IP do gateway, range IP da subnet privada, o nome que o gateway possui. É formado do FQDN precedido por um “@”, por exemplo @server.meudominio.com.br.

Primeiramente para conferir o gateway FreeSWAN, veja sua chave pública usando “ipsec showhostkey –left”. A saida deve ser algo como:

```
# RSA 2048 bits   xy.example.com   Fri Apr 26 15:01:41 2002
leftrsasigkey=0sAQOnwiBPt...
```

Se uma chave ainda não existe use o comando já visto:

```
ipsec newhostkey --output /etc/ipsec.secrets --hostname xy.example.com
```

E para verificar a chave remota, use um ssh para o servidor remoto, e digite “ipsec showhostkey –right”. a saída deve ser algo como:

```
# RSA 2192 bits   ab.example.com   Thu May 16 15:26:20 2002
```

```
rightrsasigkey=0sAQOqH55O...
```

Agora precisamos editar o arquivo /etc/ipsec.conf, e inserir a informação obtida aqui.

```
conn net-to-net
    left=192.0.2.2                # Local vitals
    leftsubnet=192.0.2.128/29     #
    leftid=@xy.example.com        #
    leftrsasigkey=0s1LgR7/oUM...  #
    leftnexthop=%defaultroute     # correct in many situations
    right=192.0.2.9               # Remote vitals
    rightsubnet=10.0.0.0/24       #
    rightid=@ab.example.com       #
    rightrsasigkey=0sAQOqH55O...  #
    rightnexthop=%defaultroute    # correct in many situations
    auto=add                      # authorizes but doesn't start this
                                  # connection at startup
```

E por fim fazer a mesma alteração no local remoto.

Assim que efetuado, você poderá levantar a conexão ipsec usando:

```
ipsec auto –up net-to-net
```

A saída será algo como:

```
104 "net-net" #223: STATE_MAIN_I1: initiate
106 "net-net" #223: STATE_MAIN_I2: sent MI2, expecting MR2
108 "net-net" #223: STATE_MAIN_I3: sent MI3, expecting MR3
004 "net-net" #223: STATE_MAIN_I4: ISAKMP SA established
112 "net-net" #224: STATE_QUICK_I1: initiate
004 "net-net" #224: STATE_QUICK_I2: sent QI2, IPsec SA established
```

Se você usa NAT ou IP Masquerade, você deverá desabilitar em ambos os gateways. E se utiliza deverá alterar para algo como:

```
iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.0/24 -d \!
192.0.2.128/29 -j MASQUERADE
```

Se um ping for efetuado, enquanto o tcpdump for executado, você poderá verificar os pacotes do ESP se movendo pela rede (*tcpdump –i eth0*):

```
19:16:32.046220 192.0.2.2 > 192.0.2.9: ESP(spi=0x3be6c4dc,seq=0x3)
19:16:32.085630 192.0.2.9 > 192.0.2.2: ESP(spi=0x5fdd1cf8,seq=0x6)
```

Mais informações sobre como implementar o FreeSWAN em uma rede poderá ser obtido em http://www.freeswan.org/freeswan_trees/freeswan-2.04/doc/.

5.4 – Cisco

5.4.1 Configurando IPSec com IKE.

Abaixo seguem os passos para uma configuração simplificada de IPSec com associações estabelecidas via IKE:

- **1 passo:** Criar uma access list para definir o trafego a ser protegido:

access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask

Exemplo:

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

Neste exemplo permite que todo trafego especificado nas condições da ALC seja protegido.

- **2 passo:** Configurar como o trafego deve ser protegido. Podemos configurar múltiplos parâmetros e habilitar um ou mais na configuração do IPSec.

```
crypto ipsec transform-set transform-set-name transform1 [transform2,
transform3]
```

Exemplo:

crypto ipsec transform-set myset1 esp-des esp-sha-hmac
crypto ipsec transform-set myset2 ah-sha-hmac esp-3des esp-sha-hmac

Neste exemplo, “myset1” and “myset2” são os nomes definidos para os parametros de configuração. “myset1” possui duas configurações definidas e “myset2” possui três configurações definidas

- **3 passo:** Criar a entrada de “crypto map”, seguindo os itens:

a. Criar a entrada de “crypto map” no IPSec utilizando o modo ISAKMP:

```
crypto map map-name seq-num ipsec-isakmp
```

Por exemplo*:*

```
crypto map mymap 10 ipsec-isakmp
```

Neste exemplo, “mymap” é o nome “crypto map” habilitadot. Este mapeamento tem um numero de sequencia 10, utilizado para realizar multiplas entradas com este parametro. Quanto menor o numero de sequencia, maior é a prioridade.

b. Associar a access list com a entrada de “crypto map”

```
crypto map map-name seq-num match address access-list-name
```

Por exemplo:

```
crypto map mymap 10 match address 101
```

No exemplo, access-list 101 é associada com a entrada de crypto map de nome “mymap.”

c. Especificar o ponto para o trafego de IPSec possa ser enviado:
```
crypto map map-name seq-num set peer ip-address
```

Por exemplo:
```
crypto map mymap 10 set peer 192.168.1.100
```

No exemplo a associação é realizada em um unico endereço ip 192.168.1.100. Pode ser especificado multiplos pontos.

d. Especificar como os parametros de configuração será feito nas entradas de crypto map. Listando os multiplos parametros de configuração na ordem de prioridade sendo a de maior prioridade primeiro. Podemos especificar seis tipos:

```
crypto map map-name seq-num set transform-set transform-set-name1
[transform-set-name2, … transform-set-name6]
```

Por exemplo:
```
crypto map mymap 10 set transform-set myset1 myset2
```

Neste exemplo, quando o trafego passar pela access list 101, a associação de segurançar “myset1” (primeira prioridade) or “myset2” (Segunda prioridade)

e. (Optional) Especificar o tempo de vida da associação de segurança par a entrada de crypto map entry, se faz se necessário se quisermos uma maior segurança e utilizarmos para a negociação diferentes tempos de SA IPSec.
```
crypto map map-name seq-num set security-association lifetime {seconds
seconds | kilobytes kilobytes}
```

Por exemplo:
```
crypto map mymap 10 set security-association lifetime seconds 2700
```

Neste exemplo um pequeno tempo de conexão foi estabelecido para a crypto map “mymap 10” em 2,700 segundos (45 minutos).

f. (Opcional) Especificar se o Ipsec pode perguntar ao PFS (Perfect forward secrecy) quando requer uma nova SA para a entrada de crypto map entry, ou pode requerer ao PFS respostas do ponto:
```
crypto map map-name seq-num set pfs [group1 | group2]
```

Por exemplo:
```
crypto map mymap 10 set pfs group2
```

Neste exemplo especifica que o PFS pode ser usado por qualquer nova negociação de SA. Para a crypto map “mymap 10.”

- **Passo 4:** Aplicar a crypto map na interface onde o trafego de IPSec será avaliado:

```
crypto map map-name interface interface-name
```

Por exemplo:

```
crypto map mymap interface outside
```

Neste exemplo, o firewall PIX deve avaliar o trafego de saida pela interface de outside que atraves da crypto map "mymap" determina o que ser necessário proteger.

- **Passo 5:** Especificar somente o trafego de IPSec implicitamente verdadeiro (permitido):

```
sysopt connection permit-ipsec
```

5.x.1 Configurando IPSec de forma manual.

- **Passo1:** Criar uma access list para definir o trafego a ser protegido:

access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask

Por exemplo

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

- **Passo 2:** Configura como trafego vai ser protegido. As AS são estabecidas manualmente

Por exemplo:

```
crypto ipsec transform-set myset3 ah-sha-hmac esp-des esp-sha-hmac
```

No exemplo, "myset3" é o nome do parametro setado e defindo 3 formas de cripgrafia.

- **Passo 3** Criar um entrada de crypto map no modo manual do IPSec:

crypto map map-name seq-num ipsec-manual

Por exemplo:

```
crypto map mymaptwo 30 ipsec-manual
```

- **Passo 4:** Aplicar a access list para o Ipsec já definida, para especificar a uma AS manual.

crypto map map-name seq-num match address access-list-name

Por exemplo:

```
crypto map mymaptwo 30 match address 101
```

- **Passo 5:** Especificar o ponto para o trafego de IPSec possa ser enviado. No modo manual somente um ponto pode ser configurado

```
crypto map map-name seq-num set peer ip-address
```

Por exemplo:
```
crypto map mymaptwo 30 set peer 192.186.1.103
```

- **Passo 6:** Especifica como os parametros podem ser utilizados.

```
crypto map map-name seq-num set transform-set transform-set-name
```

Por exemplo:
```
crypto map mymaptwo 30 set transform-set myset3
```

- **Passo 7:** È especificado as chaves utilizadas no protocolo AH (autenticação via MD5-HMAC ou SHA-HMAC), habilita o AH Security Parameter Index (SPI) e as chaves.

```
crypto map map-name seq-num set session-key inbound ah spi hex-key-data
```

Por exemplo:
```
crypto map mymaptwo 30 set session-key inbound ah 300
123456789A123456789A123456789A123456789A
```

- **Passo 8:** Habilitar as AH SPIs e chaves para aplicar no trafego de saida.

```
crypto map map-name seq-num set session-key outbound ah spi hex-key-data
```

Por exemplo:
```
crypto map mymaptwo 30 set session-key outbound ah 400
123456789A123456789A123456789A123456789A
```

- **Passo 9:** Se for especificado o ESP sera necessário configurar o ESP SPIs e chaves para o trafego de entrada.

```
crypto map map-name seq-num set session-key inbound esp spi cipher hex-
key-data [authenticator hex-key-data]
```

Por exemplo:
```
crypto map mymaptwo 30 set session-key inbound esp 300 cipher
1234567890123456 authenticator 00001111222233334444555566667777888899999
```

- **Passo 10:** Setar o trafego de ESP aplicados baseados no trafego de saida.

```
crypto map map-name seq-num set session-key outbound esp spi cipher hex-
key-data [authenticator hex-key-data]
```

Por exemplo:
```
crypto map mymaptwo 30 set session-key outbound esp 300 cipher
abcdefghijklmnop authenticator 99998888777766665555444433332222111110000
```

- **Passo 11:** Aplicar a crypto map na interface onde o trafego IPSec sera analisado:

```
crypto map map-name interface interface-name
```

Por exemplo:
```
crypto map mymaptwo interface outside
```

- **Passo 12**: Especificar somente o trafego de IPSec implicitamente verdadeiro (permitido):

```
sysopt connection permit-ipsec
```

Capítulo 6 - Bibliografias

[PLG03] Geus, Paulo Licio e Nakamura, Emilio Tissato. Segurança de Redes em Ambientes Corporativos, Editora Futura. 2003.

Domingos, João L. Segurança em Sistemas Informáticos Distribuídos. Faculdade de Ciência e Tecnologia de Lisboa

Halpern, Jason. Cisco, San Jose, CA, USA. SAFE VPN IPSec Virtual Private Networks in Depth. Novembro/2003

Figueiredo, Francisco. Acesso Remoto em Firewalls e Topologia para gateways VPN. http://bastion.las.ic.unicamp.br/paulo/papers/2001-WSeg-francisco.figueiredo-gateway.VPN.pdf, Novembro/2003.

Configuring IPSec with IKE. Cisco Systems. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/ipsec/conipsec.pdf, Outubro/2003.

IPSec User Guide for Cisco Secure Pix Firewall. http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/rel_3_0/user_gd/vc1.pdf.

Aboba, Bernand. Dixon, Willian (IPSec Working Group). IPSec-NAT Compatibility Requiriments. October 20,2003. draft-ietf-ipsec-nat-reqts-06.txt.

IPSec Protocol Overview. http://www.freesoft.org/CIE/Topics/141.htm, Novembro/2003.

White Paper IP Security for Microsoft Windows 2000 Server. Microsoft Corporation. http://www.microsoft.com/windows2000/technologies/communications/ipsec/default.asp. Novembro/2003

Kent, S; BBN Corp; Atkinson, R. RFC 2401 - Security Architecture for the Internet Protocol.

Roland, Andre; Stella, Bruno, et al. Trabalho sobre IPSec. http://www.dcc.unicamp.br/~rede10/criptografia/ipsec/, Novembro/2003.