**CONFIGURANDO UMA VPN SITE-TO-SITE (IPSEC)**

Configurar uma VPN IPSec pode não ser uma tarefa fácil. São muitos protocolos e termos envolvidos, e diversas linhas de configuração. Para facilitar um pouco essa tarefa vamos publicar alguns post (simplificando o máximo possível)sobre o assunto, sendo este primeiro post a parte teórica da coisa.

O IPSec é um framework padrão do IETF, definido pela RFC 4301, que proporciona confidencialidade, integridade e autenticação dos dados. Com o IPSec podemos criar um túnel entre dois pontos, por onde os “dados sensíveis” são enviado protegidos. Os “dados sensíveis” são definidos por quem está configurando a VPN, e normalmente são selecionados através de uma access-list.

Nos roteadores e firewalss Cisco são utilizados os seguintes protocolos, para o funcionamento do IPSec:

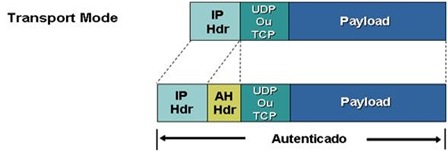
**ESP (Encapsulation Security Payload):** É um protocolo IP, tipo 50 (não é UDP nem TCP), que prove integridade, autenticação e confidencialidade dos dados. É usado para criptografar o payload dos pacotes IPs. É o principal protocolos usado pelo IPSec atualmente, e pode ser configurado no modo Túnel ou Transporte. No Túnel o pacote inteiro é encapsulado e protegido, sendo um novo cabeçalho IP adicionado ao pacote. Já no modo Transporte, são criptografados apenas os “dados”, não sendo alterado o cabeçalho original.

|  |  |
| --- | --- |
|  |  |
|  | ESP modo Túnel |

|  |  |
| --- | --- |
|  |  |
|  | ESP modo Transporte |

**AH (Authentication Header):** Semelhante ao ESP, porém não faz criptografia, e por isso em breve não será mais suportado pelos equipamentos Cisco. É o protocolo IP tipo 51 (não é UDP nem TCP), prove integridade, autenticação e replay detection. Ele é como uma assinatura digital e garante que o pacote não foi alterado. Assim como o ESP, o AH também pode ser configurado como Túnel ou Transporte. O funcionamento é igual ao do ESP.

|  |  |
| --- | --- |
|  |  |
|  | clip_image002[9] |



**Quando configurado o IPSec (com ESP ou AH) o tamanho do pacote aumenta, variando de acordo com as opções selecionadas. No máximo são adicionado 58 bytes (quando usando ESP com autenticação) por pacote.**

**IKE (Internet Key Exchange):** Protocolo hibrido que fornece para o IPSec a autenticação dos Peers, negociação do IKE e IPSec security associations, e estabelecimento de chaves que são usadas pelos protocolos de criptografias. Aparece nas configurações como ISAKMP.

**DES, 3DES e AES:** Algoritmos que fazem a criptografia dos dados. O DES utiliza chaves de 56 bits, o 3DES usa 168 bits e o AES pode trabalhar com chaves de 128, 192 e 256 bits, sendo o mais forte (também é o que consome mais processamento :)).

**DH (Diffie-Hellman):** Protocolo de criptografia com utilização de chaves públicas que foi criado em 1976 por Whitfield Diffie e Martin Hellman. O DH permite que os peers da VPN criem uma chave compartilhada (shared key) segura, mesmo sem que os peers se conheçam ou saibam da chave do ponto remoto. É usado no início do processo IKE, para estabelecer as chaves a serem utilizadas.

**MD5 e SHA-1:** Algoritmos usados para autenticar os pacotes. Para isso o SHA-1 utiliza um algoritmo que produz um “digest” de 160 bits, sendo mais seguro que o MD5, que cria um “digest” de 128 bits.

No segundo post sobre VPN, vamos identificar como ela funciona.

Uma VPN IPSec tem 5 fases: Identificação do tráfego interessante, IKE fase 1, IKE fase 2, transferência de dados e fim do túnel IPSec.

**1) Tráfego interessante:** É o tráfego que deve ser criptografado, geralmente identificado através de Access-lists.

**2) IKE fase 1:** Basicamente tem a função de negociar as políticas que serão utilizadas, autenticar os peers e fechar um túnel seguro, por onde serão configurados os demais parâmetros. Pode trabalhar em Main Mode ou Agressive Mode. Podemos dizer que é um “primeiro túnel”, para proteger as mensagens de negociação para o túnel principal.

* Main Mode: utiliza 6 troca de mensagens, e por isso é mais lento que o Agressive Mode.
* **Mensagem 1 e 2:** Usadas para garantir a segurança do meio e verificar se os peers estão de acordo.
* **Mensagem 3 e 4:** Utilizam o DH para gerar uma shared secret que é enviado para o outro peers, que devolve com sua identidade. Esta chave é usada para gerar outras chaves do processo.
* **Mensagem 4 e 5:** Faz a verificação da identidade do peer remoto.
* Agressive Mode: Utiliza apenas 3 trocas de mensagens, fazendo a identificação do peer antes de criar um canal seguro. É o modo de operação padrão.
* **Opções do IKE fase 1:**
* **Algoritmo de criptografia:** DES, 3DES, AES
* **Algoritmo Hash:** MD5, SHA-1
* **Método de autenticação:** Pré Share, RSA Signature
* **Key Exchange:** DH group 1, group 2, group 5
* **IKE SA lifetime:** até 86400 segundos

**3) IKE fase 2:** É a negociação do “segundo túnel”. São definidos os parâmetros do IPSec e transform sets, são estabelecidos IPSecs SAs, que são renegociados de tempos em tempos e pode também ocorrer a troca do DH (opcional).

O Security Association (SA) é uma conexão entre os dois peers que determina quais serviços do IPSec estão disponíveis naquela conexão (tipo de algoritmo de criptografia e autenticação utilizada, enderço IP, tempo de vida da key e outros…). São unidirecionais e assim, para um túnel VPN são criados dois SAs.

O IPSec pode trabalhar de duas madeiras: Túnel e Transporte. O modo túnel é o padrão, e com ele o pacote inteiro é criptografado e um novo cabeçalho é criado. Já no modo transporte o cabeçalho não é alterado, sendo criptografado apenas os dados.

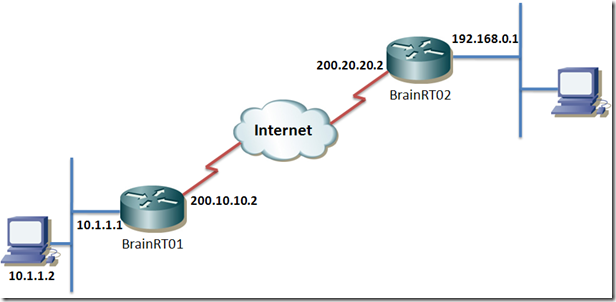
* **Opções do IKE fase 2:**
* **Algoritmo de criptografia:** DES, 3DES, AES
* **Authentication:** MD5, SHA-1
* **SA lifetime:** até 28.000 segundos

**4) Transferência de dados:** Após finalizada o IKE fase 2 o tráfego começa a ser enviado pelo túnel, de forma segura (criptografado).

**5) Fim do túnel IPSec:** O túnel é finalizado quando a SA é deletada (manualmente) ou ocorre o timeout, que pode ser configurado para ocorrer após um determinado espaço de tempo sem transmissão de dados ou após uma quantidade específica de dados transmitidos.

Continuando nossa série de posts sobre VPN IPSec, segue um exemplo da configuração passo-a-passo de uma Site-to-Site VPN, usando a **CLI** de 2 Cisco Routers, modelo 1721. O objetivo deste cenário é possibilitar o tráfego seguro (criptografado) entre as redes 10.1.1.0/24 e 192.168.0.0/24.

***Topologia:***



***Configuração do BrainRT01***

*! Primeiramente configuraremos os parâmetros ISAKMP*

*BrainRT01#conf t*

*! O número 1 é apenas o identificador da política (podemos ter mais que uma)*

*BrainRT01(config)#crypto isakmp policy 1*

*! Método de autenticação*

*BrainRT01(config-isakmp)#authentication pre-share*

*! Algoritmo de hash SHA (neste exemplo)*

*BrainRT01(config-isakmp)#hash sha*

*! Algoritmo de criptografia; neste caso, AES-128*

*BrainRT01(config-isakmp)#encryption aes 128*

*! Troca de chaves Diffie-Hellman*

*BrainRT01(config-isakmp)#group 2*

*! Tempo de vida do Security Association em segundos*

*BrainRT01(config-isakmp)#lifetime 86400*

*BrainRT01(config-isakmp)#exit*

*! Chave compartilhada para comunicação com o outro peer*

*BrainRT01(config)#crypto isakmp key Brainwork address 200.20.20.2*

*BrainRT01(config)#exit*

*! Definição dos parâmetros IKE fase 2*

*BrainRT01#conf t*

*! Criando o transform-set, onde são definidos os parâmetros usados pelo túnel IPSec, sendo ESP-AES para criptografia*

*! e ESP-SHA-HMAC para hash (MYSET é o nome do transform-set)*

*BrainRT01(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac*

*BrainRT01(cfg-crypto-trans)#exit*

*! ACL definindo qual será o tráfego protegido pelo túnel IPSec*

*BrainRT01(config)#access-list 101 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.0.255*

*! Criando o Crypto Map, que é o agrupamento das regras para construção do túnel (BrainRT01\_to\_BrainRT02 é o nome*

*! do crypto map e 10 é o identificador)*

*BrainRT01(config)#crypto map BrainRT01\_to\_BrainRT02 10 ipsec-isakmp*

*! Dentro dele, apontamos o peer remoto*

*BrainRT01(config-crypto-map)#set peer 200.20.20.2*

*! Aplicamos a ACL…*

*BrainRT01(config-crypto-map)#match address 101*

*! … e o Transform Set*

*BrainRT01(config-crypto-map)#set transform-set MYSET*

*BrainRT01(config-crypto-map)#exit*

*BrainRT01(config)#*

*! Aplicando na interface WAN de BrainRT01*

*BrainRT01(config)#interface Serial0*

*BrainRT01(config-if)#crypto map BrainRT01\_to\_BrainRT02*

*\*Mar 1 01:14:25.519: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON*

*BrainRT01(config-if)#exit*

*BrainRT01(config)#*

***Importante:*** As configurações acima postadas, devem ser aplicadas em BrainRT02 da mesma forma. As principais alterações serão nas regras da ACL e nos parâmetros que apontam BrainRT01 como peer IPSec.

Agora devemos conferir o resultado de nossa configuração. Seguem alguns comandos úteis para verificarmos o status de nosso trabalho, ou seja, o túnel IPSec “Up”:

*BrainRT01#show crypto engine connections active*

*ID Interface IP-Address State Algorithm Encrypt Decrypt*

*1 Serial0 200.10.10.2 set HMAC\_SHA+AES\_CBC 0 0*

*2001 Serial0 200.10.10.2 set AES+SHA 0 208*

*2002 Serial0 200.10.10.2 set AES+SHA 207 0*

*BrainRT01#*

*BrainRT01#show crypto session*

*Crypto session current status*

*Interface: Serial0*

*Session status: UP-ACTIVE*

*Peer: 200.20.20.2 port 500*

*IKE SA: local 200.10.10.2/500 remote 200.20.20.2/500 Active*

*IPSEC FLOW: permit ip 10.1.1.0/255.255.255.0 192.168.0.0/255.255.255.0*

*Active SAs: 2, origin: crypto map*

*BrainRT01#*