Faculdade de Engenharia da Universidade do Porto

Estudo da Viabilidade de um Serviço VPN assente numa Arquitectura Redundante

Ana Isabel Fernandes Pereira Lima

Versão Provisória

Dissertação realizada no âmbito do Mestrado Integrado em Engenharia Electrotécnica e dos Computadores
Major Telecomunicações

Orientador: Prof. João Neves

Fevereiro de 2010

Resumo

Nos dias que correm é cada vez mais frequente a necessidade de qualquer pessoa aceder a uma rede que está geograficamente distante, quer seja por motivos pessoais, quer por motivos profissionais. Para responder a esta necessidade existe a VPN, *Virtual Private Network*, que não é mais do que a criação de uma rede artificial. Desta maneira, a gestão de redes ganha importância pela necessidade de fiabilizar, proteger e garantir uma maior qualidade de serviço a esta ligação remota. Assim, a existência de uma arquitectura redundante de uma VPN ganha elevada importância na actualidade.

Abstract

Nowadays, to get access to a distant network, for personal or professional reasons, it's a very often necessity. To fulfil this request, we have VPN - *Virtual Private Network*, which consists in the creation of an artificial network. Therefore, network management gains more significance as it needs to protect, make more reliable and grant a better QoS to the established remote connection. For this reason, in these days, the existence of a VPN redundant architecture is becoming very important.

Índice

Resumo III
Abstract V
Índice VII
Lista de Figuras IX
Lista de Tabelas X
Lista de Acrónimos e Abreviaturas XI
Capítulo 1 1
Introdução 1
1.1. Natureza do Tema 1
1.2. Objectivos 2
1.3. Estruturação da Dissertação 2
Capítulo 2 3
VPNs 3
2.1. Considerações Gerais 3
2.2. Características de um Servidor de VPN 5
2.3. Requisitos de um Servidor de VPN 6
2.4. Conceitos 6
2.4.1. TCP/IP 6
2.4.2. VRRP – *Virtual Router Redundancy Protocol* 7
2.4.3. Encriptação 11
2.4.4. Túneis 12
2.4.6. IPSec 22
Capítulo 3 25
Estado da Arte 25
3.1. A Solução da Check Point - IPSec VPN *Software Blade* – Módulo de *Software* de uma VPN 26
3.2. A Solução da Juniper 28

3.3. A Solução da Cisco 32
3.3.1. Cisco ASA 5500 *Series* SSL/IPSec VPN *Edition* 32
3.3.2. IPSec VPN *Shared Port Adapter* 34
3.3.3. Cisco IOS IPSec 35
3.4. A Solução da Citrix 37
3.5. A Solução da Fortinet 38
3.6. A Solução da D-Link 39
Capítulo 4 41
Desenho da Solução Proposta 41
4.1. Cenário Um – VPN SSL *Clientless* 42
4.2. Cenário Dois – VPN IPSec Redundante (circuito) 44
4.3. Cenário Três – VPN IPSec Redundante (equipamento e circuito) 45
Capítulo 5 46
Implementação 46
Capítulo 6 59
Conclusões 59
Trabalho Futuro 61
Referências Bibliográficas 62
Anexos 64

Lista de Figuras

Figura 1 – Exemplo simplista de um cenário com VRRP. 8
Figura 2 – Exemplo de um cenário de um VR com 3 routers. 9
Figura 3 – Fluxo da transição de estados do VRRP 10
Figura 4 – Pacote IP encapsulado num Pacote IP. 12
Figura 5 – VPN *host-net* em SSH. 14
Figura 6 – VPN *host-to-net* em SSH, com IMAP. 15
Figura 7 – SSL no modelo TCP/IP. 17
Figura 8 – Camadas do SSL. 18
Figura 9 – Trama L2TP. 19
Figura 10 – Cabeçalho AH do IPSec. 22
Figura 11 – Equipamento da Juniper. 28
Figura 12 – Exemplo da Segmentação de uma rede recorrendo ao equipamento da Juniper 30
Figura 13 – Configuração de uma VPN e/ou *firewall* com redundância activo/activo. 30
Figura 14 – Serviço VPN SSL e IPSec optimizado para vários cenários de implementação. 33
Figura 15 – Alguns modelos de equipamentos da Cisco. 33
Figura 16 – IPSec VPN *Shared Port Adapter* 34
Figura 17 – Produtos Cisco capazes de fornecer um serviço VPN. 35
Figura 18 – Equipamento DFL-210. 39
Figura 19 – Vários modelos da D-Link para soluções de VPN. 40
Figura 20 – Esquema de rede do primeiro cenário – VPN SSL – *host-to-net.* 43
Figura 21 – Esquema de rede do segundo cenário – VPN IPSec Redundante – *net-to-net.* 44
Figura 22 – Esquema de rede do terceiro cenário – VPN IPSec Redundante (equipamento e circuito) – *net-to-net.* 45
Figura 23 – Esquema de rede implementado no primeiro cenário. 46
Figura 24 – Diagrama de rede testado no cenário dois. 49
Figura 25 – Laboratório de testes. 49
Figura 26 – Diagrama real de testes do cenário dois. 50
Figura 27 – Gráfico temporal relativo à conectividade através do túnel 1. 52
Figura 28 – Gráfico temporal relativo à conectividade através do túnel 2. 52
Figura 29 – Diagrama de rede testado no cenário três. 53
Figura 30 – Diagrama real de testes do cenário três. 53
Figura 31 – Gráfico temporal relativo à conectividade através do túnel 1. 56
Figura 32 – Gráfico temporal relativo à conectividade através do túnel 2. 56

Lista de Tabelas

Tabela 1 – Especificações do *software* da Check Point. 26
Tabela 2 – Desempenho da VPN em Routers e Switches Cisco. 36

Lista de Acrónimos e Abreviaturas

AH – Authentication Header

BGP – Border Gateway Protocol

CHAP – Challenge Handshake Authentication Protocol

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name Server

DSS – Digital Signature Standard

EAP – Extended Authentication Protocol

ECMP – Equal-Cost Multi-Path

ECP – Encryption Control Protocol

ESP – Encapsulating Security Payload

FEC – Forwarding Equivalence Class

FTP – File Transfer Protocol

GLBP – Gateway Load Balancing Protocol

GRE – Generic Routing Encapsulation

HMAC – Hash Message Authentication Code

HSRP – Hot Standby Router Protocol

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

IANA – Internet Assigned Numbers Authority

ICV – Integrity Check Value

IDC – International Data Corporation

IDS – Intrusion Detection System

IETF – Internet Engineering Task Force

IKE – Internet Key Exchange

IMAP – Internet Message Access Protocol

IP – Internet Protocol

IPX – Internetwork Packet Exchange

IPSec – IP Security

ISP – Internet Service Provider

JSRP – Juniper Services Redundancy Protocol

L2TP – Layer 2 Tunneling Protocol

LAN – Local Area Network

KEK – Key Encryption Keys

MAC – Message Authentication Code

MPLS – Multi Protocol Label Switching

MPPE - Microsoft Point-to-Point Encryption

MTU - Maximum Transmission Unit

NAT – Network Address Translation

NSRP – NetScreen Redundancy Protocol

OSPF – Open Shortest Path First

PAP – Password Authentication Protocol

POP3 – Post Office Protocol

PPP - Point-to-Point Protocol

PPPoE – Point-to-Point over Ethernet

PPTP – Point-to-Point Tunneling Protocol

RAS – Remote Access Server

RIP – Routing Information Protocol

RSA – Ronald Rivest, Adi Shamir, Leonard Adleman

SMLT – Split Multi-Link Trunking

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Managemant Protocol

SSH – Secure Shell

SSL – Secure Sockets Layer

TCP/IP – Transmission Control Protocol / Internet Protocol

TELNET – Teletype Network

TLS – Transport Layer Security

UDP – User Datagram Protocol

VoIP – Voice over I*P*

VPN – Virtual Private Network

VRRP – Virtual Router Redundancy Protocol

WAN – Wide Area Network

Capítulo 1

Introdução

Este primeiro capítulo tem por função mostrar a forma como o trabalho foi desenvolvido e escrito nesta dissertação, explicando a natureza do tema e o que se pretende com este estudo. Ainda neste capítulo são nomeados os objectivos propostos e explicada a forma como esta dissertação está organizada.

1.1. Natureza do Tema

Um serviço de VPN (*Virtual Private Network*) é um serviço que oferece uma rede segura sobre um conjunto de redes que se pressupõem potencialmente inseguras. Esta rede é chamada de virtual porque liga duas redes locais (LAN), separadas fisicamente, através de um ambiente inseguro, a Internet. Uma vantagem deste serviço de VPN é o custo reduzido. No entanto a qualidade de serviço de uma VPN é menor comparada com uma ligação por um circuito dedicado, na medida em que uma VPN usa a rede pública.

Assim, aparece a obrigatoriedade de garantir uma elevada qualidade de serviço, mas a preços reduzidos. Para solucionar esta limitação surge a necessidade de uma redundância. Ou seja, se for projectada uma VPN com ligações redundantes, o serviço já tem maior qualidade e fiabilidade. Mesmo usando a Internet para se aceder a uma rede remota pode ter-se garantia de quebras mínimas de serviço se for implementada a redundância da ligação.

1.2. Objectivos

Nesta dissertação pretende-se estudar a possibilidade e a viabilidade de um serviço VPN que assente numa arquitectura redundante com dois ou mais servidores. Ou seja, caso haja uma quebra na ligação da VPN, o utilizador dessa mesma VPN continuará a usufruir deste serviço, pela redundância criada na rede.

Para a execução desta dissertação propõe-se estudar os requisitos necessários para o seu desenvolvimento, investigar e seleccionar os protocolos possíveis para esta solução.

Um objectivo deste trabalho é o desenvolvimento de um esquema de ligações desta solução, com ou sem arquitectura redundante, implementando e testando o esquema elaborado e as suas respectivas configurações.

No final deste estudo, pretende-se demonstrar a viabilidade desta solução, explicando as conclusões inerentes a todo o seu desenvolvimento.

1.3. Estruturação da Dissertação

Esta dissertação está dividida em seis partes. A primeira parte é a introdução da dissertação, em que temos um breve enquadramento do tema, a definição dos objectivos e a explicação de como a dissertação está organizada. A segunda parte, ou o capítulo 2, faz uma introdução às VPNs, onde são explicados conceitos chave e onde são apresentados vários tipos de VPNs. O terceiro capítulo dá-se pelo nome de “Estado da Arte” e prende-se com um estudo de mercado, descrevendo as soluções disponibilizadas pelos fabricantes desta tecnologia. O capítulo 4,”Desenho da Solução Proposta”, mostra os diferentes esquemas de rede que são propostos para implementação. O capítulo seguinte, “Implementação”, demonstra tudo o que foi implementado e testado em laboratório. O capítulo sexto é onde são postas as conclusões desta dissertação, resumindo todo o seu desenvolvimento. De seguida apresenta-se o “Trabalho Futuro”, em que são apontados os desafios para uma futura continuação deste desenvolvimento. As “Referências Bibliográficas” referem todos os locais de pesquisa necessários para a elaboração desta dissertação. E finalmente, surgem os “Anexos” que são referenciados neste trabalho.

Capítulo 2

VPNs

2.1. Considerações Gerais

Hoje em dia a Internet é parte integrante das comunicações de uma organização. Quer as empresas, governo ou instituições usam a Internet como uma extensão das suas redes informáticas.

A Internet é um meio de fácil acesso, estável e barato, contudo pouco seguro, pelo menos na sua essência.

Qualquer utilizador pretende que toda a sua informação confidencial não esteja disponível a terceiros, como códigos de acesso à banca *on-line*, dados pessoais ou informações confidenciais de empresas.

Deste modo, o utilizador pretende que toda a informação atravesse a Internet, da origem ao seu destino, através de um canal privado, sem qualquer "entropia".

Tendo a Internet o protocolo TCP/IP por base, e sendo este protocolo pouco seguro, surgem então as VPNs. Este conceito fornece a segurança pretendida e possível, assim como uma série de outras funcionalidades.

A segurança permite o desenvolvimento da economia da Internet e é um componente fundamental de qualquer estratégia de *e-business* (negócio electrónico). À medida que os gestores de rede de uma empresa abrem as suas redes a um número crescente de utilizadores e aplicações, estão a expor as suas redes a um risco acrescido. As organizações correm riscos e plataformas como as *firewalls*, sistemas de detecção de intrusão (IDS) e produtos para VPNs asseguram uma implementação segura e bem sucedida de soluções *e-business,* bem como soluções de redes corporativas.

Uma VPN consiste em diversas soluções de comunicação segura. É um prolongamento seguro de uma rede privada sobre uma rede insegura, normalmente pública. Criar uma VPN significa gerar um ambiente de rede seguro sobre um grupo de redes que podem ser inseguras.

Os avanços tecnológicos de hoje conduziram a que instituições ou empresas interligassem as suas delegações através da tecnologia VPN. Um sistema de comunicação por VPN tem um custo de implementação e manutenção insignificantes, se comparados aos antigos sistemas de comunicação física, como por exemplo, o *Frame relay*. Para além do custo baixo, as VPNs disponibilizam um elevado grau de operacionalidade e integridade dos dados transferidos.

Actualmente, as VPNs estão a atingir uma forte divulgação, visto que a grande maioria dos equipamentos instalados pelos fornecedores de Internet (ISP – *Internet Service Provider*) já estão munidos desta e de outras tecnologias, que tornam os dados dos utilizadores menos vulneráveis.

As *secure* VPN, VPNs seguras, garantem que a segurança dos dados entre a origem e o destino não depende do encaminhamento, nem da integridade dos fabricantes. É uma solução escalonável que tem tido maior aceitação por parte das empresas e dos clientes residenciais.

As *trusted* VPN, VPN confiáveis, não são flexíveis. Asseguram que o encaminhamento dos dados numa rede pública não dependerá dos fornecedores, quer seja no acesso, quer seja no caminho, com excepção dos fornecedores que a origem pode confiar.

Uma VPN é uma ligação de rede virtual que proporciona uma ligação externa a uma rede segura. Para que isto possa ser feito com a fiabilidade existente e necessária, temos que garantir segurança na comunicação de dados. Os dados têm de manter a integridade e confidencialidade durante a passagem na rede "insegura".

As chaves de sessão são indispensáveis para a segurança das VPNs. Estas chaves são valores secretos e iguais, que são partilhados por um certo grupo de envolventes, normalmente origem e destino. As chaves de sessão são definidas no início dessa sessão pelas partes envolventes, e são descartadas logo que a sessão terminar.

Existem diversas formas de negociar chaves de sessão e cada VPN opta pela sua. Geralmente estas chaves são de longa duração para que a protecção dos dados seja feita durante toda a ligação, e são conhecidas como KEK (*Key Encryption Keys*).

As KEK, chaves de encriptação de chaves, podem ser de dois tipos. Um tipo de chave é simétrica, secreta e partilhada entre as duas partes da negociação. O outro tipo de chave é um par de chaves assimétricas por cada parte da negociação.

As VPNs podem ser de dois tipos: *host-to-net* e *net-to-net*.

Uma VPN *host-to-net* permite que uma máquina que esteja fisicamente externa a uma rede aceda a essa mesma rede. Pode-se imaginar um colaborador de uma empresa, que está na sua casa ou num *cybercafe*, e pretende aceder à rede da sua empresa. Esta solução permite acabar com as limitações geográficas.

Uma VPN *net-to-net* tem como objectivo unir as diversas redes que possam estar dispersas geograficamente. Tome-se como exemplo uma empresa com diversas filiais, espalhadas geograficamente, mas que partilhem recursos.

No passado as VPNs *net-to-net* apenas eram possíveis através de circuitos dedicados, o que as tornava dispendiosas. Hoje em dia, pode-se usar a Internet ou, por exemplo, o serviço IP MPLS para esse mesmo fim. Ou seja, torna-se possível usufruir das vantagens deste tipo de VPN a um custo baixo.

Para que se estabeleça uma VPN passa-se por um processo de autenticação, quer de pessoas, quer de máquinas. Quando se estabelece uma VPN *host-to-net* pode autenticar-se o utilizador da máquina ou a própria máquina, independentemente de quem a usa. Numa VPN *net-to-net* é feita a autenticação das máquinas ou dos serviços.

A implementação de uma VPN necessita de túneis seguros (*secure tunneling*) ou de encapsulamento seguro (*secure encapsulation*). Um túnel seguro é uma forma segura para encapsular acções remotas na VPN. Através do encapsulamento seguro prevenimos que alguém consiga perceber que tipo de acções estão a decorrer na VPN.

Os túneis podem ser implementados de forma evidente ou de forma transparente. Quando um túnel é implementado de forma evidente, o utilizador da VPN tem de direccionar as suas acções para o mecanismo controlador de um dos pontos extremos do túnel. Se o túnel for implementado de forma transparente, o utilizador não tem qualquer condicionalismo nas suas acções. A diferença entre a utilização segura ou transparente de um túnel reside no nível protocolar em que o túnel da VPN é estabelecido. Se o túnel for executado de forma transparente então é realizado pelos sistemas operativos abaixo da camada de transporte, inclusive. Se o túnel for estabelecido de forma evidente então é realizado na camada das aplicações, acima da camada de transporte.

2.2. Características de um Servidor de VPN

Um servidor de VPN tem de possuir algumas características que se tornam essenciais para um bom serviço.

Uma das características de um servidor de VPN é ser capaz de fornecer segurança através da encriptação dos dados ponto-a-ponto.

A garantia da integridade dos dados é um ponto importante para um servidor de VPN, ou seja, os dados não serão modificados durante o seu caminho.

Para que haja segurança, o servidor tem de ser possuidor de autenticação da origem, para que apenas os utilizadores autorizados possam aceder.

O servidor de VPN tem de dispor de capacidade para permitir o acesso a clientes remotos autorizados aos recursos da LAN corporativa, mas também de viabilizar a interligação de LANs de forma a possibilitar o acesso a filiais, partilhando recursos e informações.

2.3. Requisitos de um Servidor de VPN

Um servidor VPN tem de obedecer a alguns requisitos para que todo o seu funcionamento corra na perfeição.

Um dos requisitos é a autenticação dos utilizadores, onde é feita a verificação da identidade do utilizador, restringindo o acesso a autorizados. O servidor deve dispor de mecanismos de registo referente aos acessos efectuados (quem acedeu, o que foi acedido, quando foi acedido).

A gestão de endereços é mais um requisito. O endereço origem (do utilizador) não deve ser divulgado na sua rede privada, deve-se adoptar endereços fictícios para o tráfego externo.

Mais um requisito necessário é a encriptação de dados. Os dados devem percorrer a rede pública ou privada num formato encriptado e, caso sejam interceptados por utilizadores não autorizados, não deve ser possível a sua descodificação, garantindo a privacidade da informação.

O uso de chaves que garantem a segurança dos dados encriptados deve operar como uma palavra-chave partilhada exclusivamente entre as partes envolvidas. A gestão de chaves deve garantir a troca periódica das mesmas, visando manter a comunicação de forma segura.

Um servidor tem de ser capaz de suportar múltiplos protocolos. Com a diversidade de protocolos existentes, torna-se bastante desejável que a VPN suporte protocolos *standard* usados nas redes públicas, tais como, IP (*Internet Protocol*) ou o IPX (*Internetwork Packet Exchange*).

2.4. Conceitos

2.4.1. TCP/IP

Todo o encaminhamento e fluxo de informação gerada e transportada pela Internet são controlados por um conjunto de protocolos, denominado por TCP/IP. No seu conjunto forma a infra-estrutura usada pelas aplicações para que estas comuniquem entre si, quer entre máquinas da mesma rede local, quer entre máquinas de todo o mundo.

O TCP é um protocolo usado para transmissão de dados de uma aplicação para a rede, sendo responsável pela comunicação entre o *software* de aplicação (*browser*) e o *software* de rede, enquanto o IP cuida da comunicação entre as máquinas da rede.

O TCP é responsável, não só por fragmentar os pacotes IP antes de serem enviados, mas também por juntá-los quando chegam ao destino. O IP é um protocolo que se preocupa em enviar os pacotes para o destino correcto.

TCP/IP é uma grande combinação de protocolos de comunicação, organizados numa pilha. Esta pilha é um modelo de cinco camadas, em que cada camada tem a sua função: física, ligação de dados, rede, transporte e aplicação.

A camada física do modelo TCP/IP diz respeito ao hardware, ou seja, aos meios de conexão de duas interfaces, entre as quais haverá tráfego de dados.

A camada *data link*, ligação de dados, é responsável pela transmissão e recepção de tramas, assim como pelo fluxo de dados. A ligação envolve os componentes físicos e lógicos utilizados para interligar os utilizadores e os nós da rede. O protocolo de ligação é um conjunto de métodos que operam apenas entre nós de rede adjacentes de um segmento de LAN ou de uma conexão de WAN.

A camada de rede (camada de Internet) é responsável pelo *routing* de um pacote da sua rede de origem para a sua rede de destino, ou seja, esta camada resolve o problema do envio de pacotes através de uma ou de mais redes.

A camada de transporte é responsável pela entrega de mensagens *end-to-end* independentemente da rede em que circulam, com as funcionalidades de controlo de erros, de segmentação, de controlo de fluxo, de controlo de congestionamento e endereçamento aplicacional (números de portos).

A camada de aplicação refere-se aos protocolos de nível mais elevado utilizados nas aplicações para a comunicação de rede.

2.4.2. VRRP – *Virtual Router Redundancy Protocol*

Em redes com um elevado números de sites, os protocolos de *routing* dinâmico, como por exemplo o RIP, o BGP ou o OSPF, são muitas vezes usados. Contudo existem factores que por vezes não os tornam desejáveis. Uma alternativa é a configuração de rotas estáticas, todavia se o primeiro salto falha, deixamos de poder comunicar para o exterior.

O protocolo VRRP (*Virtual Router Redundancy Protocol*) fornece uma solução viável, através da agregação de routers num grupo lógico designado por *Virtual Router* – VR.

O VRRP é o protocolo *standard* (padrão) deste tipo de tecnologia, patente na RFC 2338. No entanto, existem protocolos proprietários, como por exemplo o SMLT da Nortel e o HSRP e o GLBP da Cisco.

Destes protocolos existe uma elevada semelhança entre o VRRP e o HSRP. A particularidade do GLBP é o de permitir o balanceamento do tráfego na saída, ou seja, ambas as *gateways* da rede transportam tráfego de entrada e saída. No VRRP e no HSRP apenas uma *gateway* ficará com a função de transportar o tráfego de entrada e de saída, enquanto que a outra *gateway* fica em *backup*.

A principal função do VRRP é comunicar com todos os routers associados através do *Virtual Router* ID, bem como promover a redundância através da eleição de um deles pela prioridade mais alta. Cada router terá configurado o mesmo endereço IP virtual, contudo apenas um será o *owner* (dono) desse endereço na realidade. O equipamento em que é configurada a prioridade mais elevada é o *owner*. Os outros routers com prioridades inferiores ficam a operar como *backup* até que o *owner* permaneça operacional.

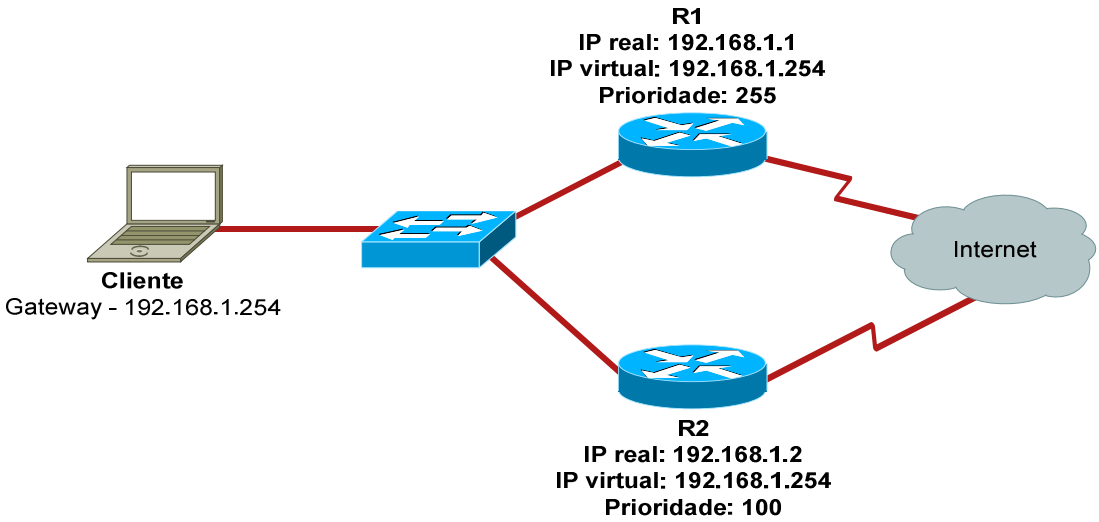


Figura 1 – Exemplo simplista de um cenário com VRRP.

O *owner* geralmente opera como *Master Router* do VR. No entanto, quando este fica inoperacional, ocorre o processo de eleição, e o *Backup Router* torna-se *Master*.

Todos os routers pertencentes ao mesmo VR têm de estar configurados com o mesmo *advertisement time*. O *advertisement time* é o intervalo de tempo em que o router alerta os restantes membros do VR que está operacional. Caso esse intervalo não corresponda, o router irá descartar o pacote.

Os pacotes do protocolo VRRP são encapsulados no pacote IP e são enviados para o endereço *multicast* IPv4. O endereço IP de *multicast* definido pela IANA para o VRRP é o 224.0.0.18 e o número associado ao protocolo é o 112.

A nível da segurança, o router irá descartar qualquer pacote do VRRP senão possuir o TTL a 255, ou seja, limita as vulnerabilidades a ataques na rede local pois caso sejam injectados pacotes de outra rede remota o TTL é alterado. Num pacote IP o TTL é reduzido a menos uma unidade cada vez que atravessa um router.

O *Virtual Router* (VR) é um conjunto de routers, constituído por um router *Owner* e por um ou mais routers *Backup*, pertencentes à mesma rede local.

Cada VR tem um diferente VRID (*Virtual Router Identifier*). Os routers de cada VR têm o mesmo VRID configurado, assim como o mesmo endereço IP virtual. Cada VR tem apenas um *Owner*.

O VRRP atribui automaticamente o endereço MAC à interface, baseando-se no prefixo padrão para os pacotes do VRRP e do VRID. Os primeiros cinco octetos são 00:00:5E:00:01 e último octeto é o VRID configurado.

O IP virtual associado ao VR deverá ser igual em todos os routers. Contudo todos os routers têm da mesma forma um IP real configurado, pertencente à mesma *subnet* da rede local.

O router *Master* responde a pedidos ARP com o endereço MAC atribuído pelo VR, e é também usado como sendo o endereço origem na divulgação de pacotes pelo *Master*. Os routers *Backup* não respondem a pedidos ARP do IP virtual.

Na figura seguinte pode ver-se um exemplo de um VR com 3 routers.

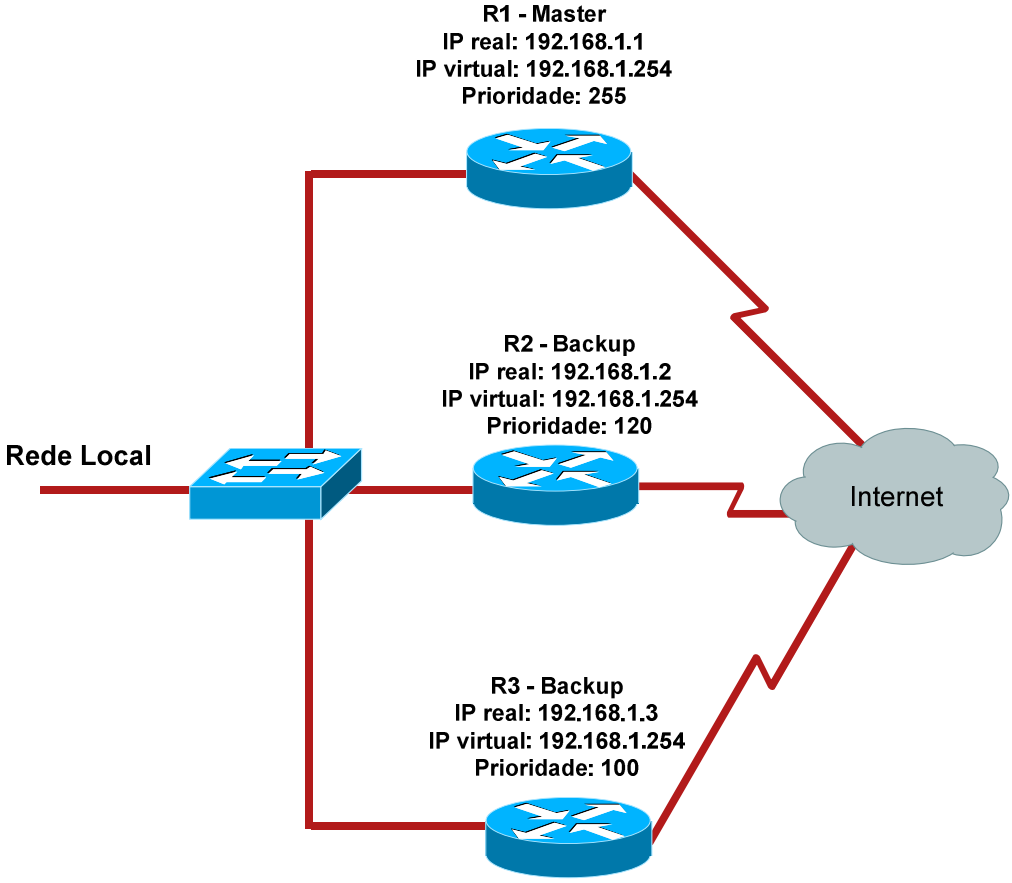


Figura 2 – Exemplo de um cenário de um VR com 3 routers.

No exemplo da figura 2, o R1 é o *Owner*, a prioridade está definida com o valor 255. Nos restantes membros do VR, os endereços IP reais são diferentes entre si e diferentes do IP virtual.

A vantagem desta solução é a flexibilidade da rede. Como o IP virtual não é igual ao IP real, os routers podem ser alterados fisicamente, bem como os seus endereços sem a necessidade de reconfigurar o router virtual.

Num VR o router *Master* opera como a *gateway* física da rede. A eleição do router *Master* é controlada pelo valor da prioridade. Na figura 2, o router R1 é o router *Master* pois apresenta uma prioridade superior dos restantes. Quando o router R1 fica inoperacional o router R2 assume o comando, pois o valor da prioridade de R2 é superior ao valor da prioridade de R3, contudo estes valores são inferiores è prioridade de R1.

Um VR terá de conter pelo menos um router *Backup*. Neste router deverá ser configurado o mesmo IP virtual do router *Master*. A prioridade por defeito é 100. Quando o router *Master* volta a estar operacional, assume o papel de *gateway* da rede novamente. Caso não se pretenda que isso aconteça, o modo *preempt* deve estar desactivo.

Cada *Virtual* Router pode assumir três estados: *Init*, *Backup* e *Master*.

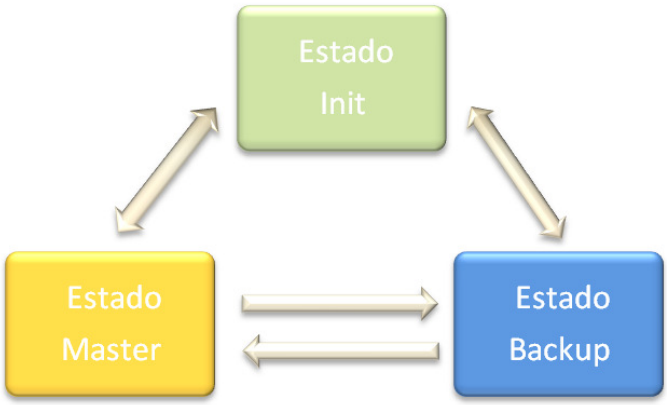


Figura 3 – Fluxo da transição de estados do VRRP.

A finalidade do estado *Init* é aguardar pelo evento de *Startup*. Quando o router recebe este evento, verifica se a prioridade é de 255. Em caso afirmativo, é enviado o *advertisement packet* e os pedidos ARP de *broadcast*, passando o seu estado para *Master*. Em caso negativo, o estado passa para *Backup*.

No estado *Backup*, o router não responde a pedidos ARP e não manda tráfego para o IP associado com o VR. Os routers, neste estado, receberem os *advertisement packets* e verificam se o router *Master* está operacional.

Se um router estiver no estado *Backup* e se a prioridade de um *advertisement packet* é 0 ou caso o modo *preempt* esteja desactivo ou a prioridade de *advertisement* é maior ou igual à prioridade local, os routers *Backup* enviam *advertisement packets*, pedidos ARP de *broadcast* e transitam para o estado *Master*. Nos casos restantes, os *advertisement packets* serão descartados. Se um router receber o evento de *shutdown*, ocorre a transição para o estado *Init*.

Quando o router se encontra no estado *Master*, responde a pedidos ARP e encaminha o tráfego para o endereço IP associado ao VR. O router *Master* envia *advertisement packets* nos intervalos de tempo definidos na configuração do VRRP.

No caso de um router estar no estado de *Master*, e recebe um *advertisement packet* em que a prioridade é igual a 0, a resposta é imediatamente enviada. No caso da prioridade ser maior, o router transita para o estado *Backup*. No caso da prioridade ser igual e o endereço IP real for maior que o endereço IP local, então o router transita para o estado *Backup*. Nos restantes casos os *advertisement packets* são descartados.

Ainda referente à figura 2, apresenta-se um exemplo de configuração:

R1 (*Master*)

```
interface F1/0
 ip address 192.168.1.1 255.255.255.0
 vrrp 1 description GRUPO_VRRP_1
 vrrp 1 ip 192.168.1.254
 vrrp 1 priority 255
 vrrp 1 preempt
 vrrp 1 timers advertise 3
 no shutdown
```

R2 (*Backup*)

```
interface F1/0
 ip address 192.168.1.2 255.255.255.0
 vrrp 1 description GRUPO_VRRP_1
 vrrp 1 ip 192.168.1.254
 vrrp 1 priority 120
 vrrp 1 preempt
 vrrp 1 timers advertise 3
 no shutdown
```

R3 (*Backup*)

```
interface F1/0
 ip address 192.168.1.3 255.255.255.0
 vrrp 1 description GRUPO_VRRP_1
 vrrp 1 ip 192.168.1.254
 vrrp 1 preempt
 vrrp 1 timers advertise 3
 no shutdown
```

Na configuração apresentada pode ver-se que o R1 é o router *Master* e que o endereço IP virtual deste VR é 192.168.1.254. O R2 ficará como primeiro *backup* pois apresenta uma prioridade inferior ao R1 mas superior ao R3, que ficará como segundo *backup* deste grupo de VRRP. Como o modo *preempt* está configurado, caso R1 fique inoperacional, o R2 assumirá o estado *Master.*

2.4.3. Encriptação

A encriptação de dados é um processo de transformar a informação usando um algoritmo para que se torne inacessível a todos, com excepção daqueles que souberem a *key* (chave).

Este algoritmo usado é geralmente chamado de cifra. Uma cifra não é mais do que um conjunto de tópicos bem definidos que podem ser seguidos como um procedimento.

A chave é um bocado de informação que define o resultado de um algoritmo ou de uma cifra. Uma chave especifica a transformação de texto legível em texto cifrado, e em processo inverso.

O resultado deste processo é a informação encriptada. A desencriptação também está patente neste processo, para que as informações se voltem a ler.

O processo de encriptação é usado para proteger os dados que estejam a ser transmitidos pela rede, assim como para combater o acesso indesejado à rede.

A encriptação pode proteger a confidencialidade das mensagens, mas são necessários outros métodos para assegurar a integridade e a autenticidade das mensagens. Estes métodos podem ser, por exemplo, a verificação de um código de autenticação de mensagem (MAC- *Message Authentication Code*) ou uma assinatura digital.

Um MAC é um bocado de informação que é usada para autenticar uma mensagem. O algoritmo de MAC aceita como entrada uma chave secreta e uma mensagem de comprimento variável para serem autenticados, e como saída um MAC. O MAC protege a integridade e a autenticidade de uma mensagem de dados, pela existência de verificadores das alterações do conteúdo da mensagem.

A assinatura digital é um esquema matemático para demonstrar a autenticidade de uma mensagem digital. Se a assinatura digital for válida, então pode-se acreditar que esse está perante uma mensagem com um remetente válido, e que esta mensagem não foi alterada durante a sua transmissão. As assinaturas digitais costumam ser usadas em aplicações financeiras, na distribuição de *software* e em casos que seja importante detectar que os documentos possam ter sido alterados.

2.4.4. Túneis

Os túneis são criados, de uma maneira geral, para formar uma rede virtual que assenta sobre uma rede física.

Existem vários tipos de túneis, como por exemplo: IP em IP, PPPoE, GRE, PPTP, L2TP, MPLS.

Os túneis IP-IP regem-se por um protocolo de *tunneling* que encapsula um pacote IP num outro pacote IP. Para que este encapsulamento seja possível, é adicionado ao pacote IP um outro *header*. Este *header* terá informação do *source* IP, do ponto de entrada no túnel, do ponto de destino e do ponto de saída do túnel.

Com a adição deste *header*, o pacote IP não é alterado, apenas o campo TTL é decrementado. Mas se o tamanho do pacote é maior que o *path* MTU, o pacote é fragmentado na sua origem com o novo cabeçalho incluído. No destino, o pacote volta a unir-se.

Na figura seguinte podemos ver o novo cabeçalho que é adicionado ao pacote IP:

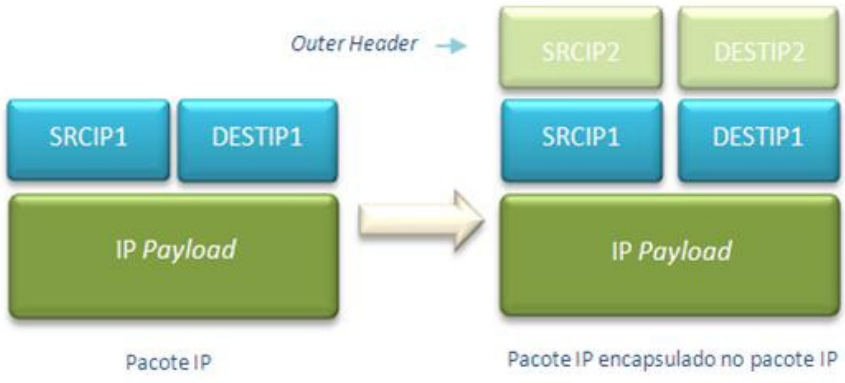


Figura 4 – Pacote IP encapsulado num Pacote IP.

O GRE (*Generic Routing Encapsulation*) é um protocolo de *tunneling*, desenvolvido pela Cisco, que tem a capacidade de encapsular vários tipos de pacotes de diversos protocolos de rede dentro de túneis IP. Assim, é criada uma ligação virtual ponto-a-ponto, túnel GRE, em que não se sabe o estado de nenhuma das duas extremidades do túnel. Um cabeçalho GRE permite descrever um encapsulamento genérico.

O protocolo PPTP (*Point-to-Point Tunneling Protocol*) é usado para implementar VNPs. Este protocolo permite encriptar e encapsular tráfego, de diversos protocolos, usando um cabeçalho IP. Para que haja transmissão, o PPTP encapsula tramas PPP em datagramas IP, usando uma conexão TCP para gestão do túnel. Este protocolo será mais desenvolvido na seccção da VPN PPTP.

Os túneis PPPoE (*Point-to-Point over Ethernet*) são capazes de encapsular uma trama PPP dentro de uma trama *Ethernet*. Os pacotes *Ethernet* contêm o endereço de hardware (MAC *address*) do nó de destino, o que facilita no caminho para o destino pretendido. Um túnel PPPoE é um túnel que interliga directamente duas máquinas através de uma rede *Ethernet*.

O protocolo L2TP (*Layer 2 Tunneling Protocol*) é um protocolo de encriptação, que recorre a túneis para oferecer privacidade. Os túneis L2TP podem ser formados numa sessão PPP ou numa parte da sessão apenas.

As extremidades de um túnel L2TP são conhecidas por LAC (L2TP *Access Concentrator*) e por LNS (L2TP *Network Server*). O LAC é responsável por iniciar o túnel e o LNS é o servidor que espera por novos túneis. Num túnel L2TP o tráfego é bidireccional. Os pacotes trocados num túnel L2TP são classificados como pacotes de controlo ou pacotes de dados.

Podemos ter quatro tipos de túneis L2TP: *voluntary tunnel*, *compulsory tunnel* (*incoming call*), *compulsory tunnel* (*remote dial*) e conexão *multi-hop* L2TP. Um *voluntary tunnel* é um túnel voluntário, ou seja, sem qualquer intervenção do provedor de acesso. Um *compulsory tunnel* (*incoming call*), um *compulsory tunnel* (*remote dial*) e uma conexão *multi-hop* L2TP são modos de *tunneling* em que o provedor do acesso verifica as credenciais para o estabelecimento do túnel L2TP. Este protocolo será mais desenvolvido na secção da VPN L2TP.

O MPLS (*Multiprotocol Label Switching*) é mais um protocolo de *tunneling*, que faz o transporte de dados, operando entre a camada de dados e a camada de rede.

Quando um pacote sem etiqueta entra num router de acesso e necessita de passar num túnel MPLS, o router determina o FEC (*Forwarding Equivalence Class*) do pacote e insere uma ou mais etiquetas no *header* MPLS que foi criado para o efeito. Quando este pacote sai do túnel MPLS, este *header* é removido. O MPLS utiliza *label stacking* (empilhamento de etiquetas) para poder suportar túneis de conexões dentro de conexões.

2.4.5. Vários Tipos de VPNs

2.4.5.1. VPN SSH

O SSH (*Secure Shell*) é uma aplicação capaz de estabelecer sessões seguras, mas também poderá ser um protocolo de rede. Estas sessões são seguras sobre uma ligação segura, como por exemplo, uma sessão de FTP (*File Transfer Protocol*) ou uma sessão de TELNET.

Existem duas versões do protocolo SSH, sendo mais aconselhável a segunda versão por ser menos vulnerável, visto que tem mais algoritmos de autenticação e mais algoritmos para a cifra de conteúdos.

Pode estabelecer-se um canal de comunicação seguro sobre uma ligação TCP que suporta diferentes fluxos de transporte, através de uma ligação segura SSH. Na camada de transporte há uma multiplexagem de diversos fluxos TCP que permite estabelecer túneis seguros, dando origem a uma VPN *host-to-net*.

A figura seguinte mostra a forma como se pode estabelecer uma VPN *host-to-net* através da aplicação SSH.

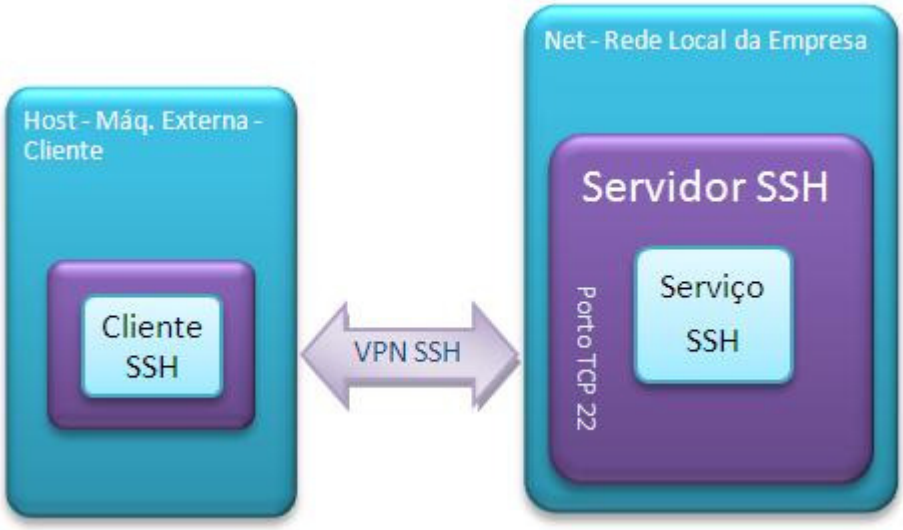


Figura 5 – VPN *host-net* em SSH.

De um lado temos a máquina (*host*), que está externa à rede, e do outro lado temos, por exemplo, a rede de uma empresa, à qual o *host* pretende aceder. Na rede da empresa existe uma máquina *SSH_server* que é responsável por executar o serviço de VPN SSH (*SSH daemon*). O serviço de VPN SSH permite que sejam criadas ligações seguras SSH ao *host*, depois do utilizador (*host*) ser autenticado e autorizado. Geralmente, as ligações seguras usam o porto TCP 22. Quando uma ligação segura SSH é estabelecida por um *host* fora da rede da empresa, então é criada uma VPN para essa mesma rede, com recurso à máquina *SSH_server*.

Pressupondo que foi estabelecida uma ligação segura SSH entre a máquina externa, *host*, e a máquina *SSH_server*, o utilizador pode estabelecer túneis seguros (*secure tunneling*). Estes túneis seguros são feitos pelo mapeamento entre os portos TCP da sua máquina (cliente) e os portos TCP/IP da rede, executado na aplicação cliente SSH. Os túneis seguros podem ser de entrada (*incoming tunnel*) ou de saída (*outgoing tunnel*).

Um cliente SSH pode definir perfis de ligação segura, permitindo associar ligações seguras a certos túneis seguros.

Um túnel é chamado "de saída" porque se considera o ponto de vista do utilizador que o estabelece. O *outgoing tunnel* redirecciona as ligações TCP, que o utilizador estabelece, para uma máquina dentro da rede da empresa.

Supondo que foi estabelecido um túnel seguro de saída, onde está mapeado o porto TCP x na máquina cliente para o porto TCP y de uma máquina z na rede da empresa, o cliente SSH abre o porto x para ligações de aplicações de clientes.

Assumindo que é executada uma aplicação cliente na máquina *host* e que é estabelecida uma ligação para o porto TCP x, o cliente SSH vai pedir ao *SSH daemon* (ponto extremo da ligação segura SSH residente no *SSH_server*) que estabeleça uma ligação para o porto TCP y da máquina z. Consequentemente, a aplicação cliente comunica com o porto TCP y da máquina z por um túnel seguro.

A próxima figura mostra um exemplo da aplicação de um túnel seguro SSH. Um utilizador externo quer aceder à sua caixa de correio através do servidor de IMAP, residente na rede da empresa.

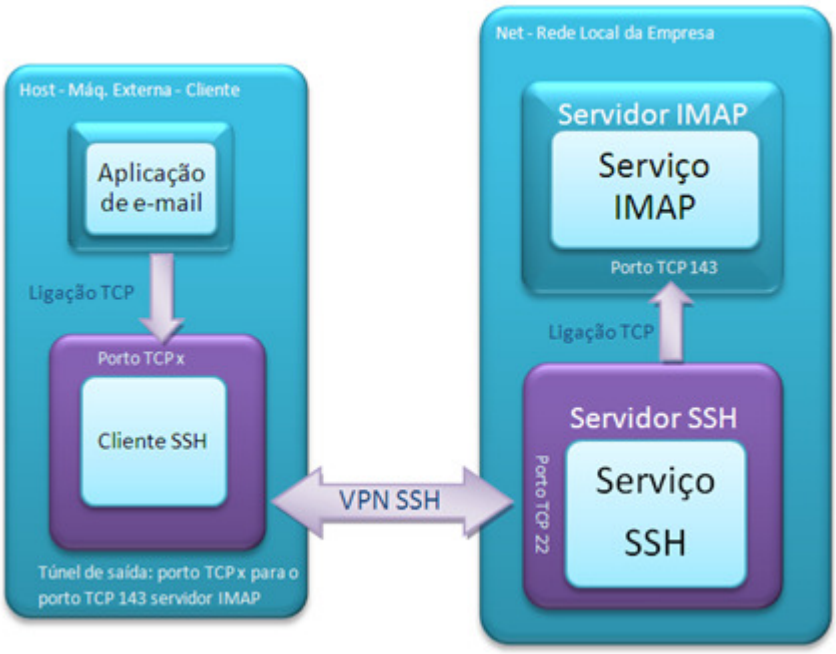


Figura 6 – VPN *host-to-net* em SSH, com IMAP.

Como o protocolo IMAP não tem qualquer tipo de protecção de dados, determina-se que o acesso ao servidor IMAP do exterior tem que utilizar um túnel SSH seguro. O servidor de IMAP não é acedido directamente de fora da rede da empresa porque esta mesma rede apenas possui um IP público que é utilizado pelo servidor SSH.

Como tal, o utilizador define na aplicação cliente um túnel seguro sobre SSH, em que especifica que o túnel tem de ser estabelecido sobre uma ligação segura para o *SSH_server*, e tem de mapear o porto TCP x para o porto IMAP TCP 143 no servidor IMAP. Depois de activa a ligação segura SSH, o porto x aparece na máquina do utilizador externo. A aplicação que acede à caixa do correio no utilizador externo tem que ser configurada para que aceda à aplicação que está no porto TCP x (*SSH_server*). E finalmente, o utilizador pode aceder à sua caixa de correio como normalmente o faz.

Se um servidor SSH tiver um IP público e permissões de estabelecimento de túneis seguros, será garantido um acesso seguro a servidor com um IP privado.

As VPN SSH são evidentes (e não transparentes) porque têm de ser definidos mapas para os túneis seguros e as aplicações, que estão envolvidas com o túnel seguro, têm de ser configuradas para que comuniquem com o porto TCP do cliente SSH.

Um túnel "de entrada" requer um mapeamento numa ligação segura SSH, entre um porto TCP local ao serviço SSH e um porto TCP/IP remoto. Estes túneis são responsáveis pelo fluxo de dados TCP de dentro da rede privada para o exterior, sem que possibilitem qualquer acção iniciada no exterior da rede.

Um exemplo de uma ligação iniciada na rede protegida para uma máquina no exterior é a transferência de dados FTP. O cliente FTP configura como porto TCP/IP para receber os dados, o porto onde está o serviço SSH, ou seja, o porto de entrada do túnel. De seguida, o cliente FTP espera por uma ligação TCP originada pelo cliente SSH.

Existem ainda os túneis dinâmicos, que são utilizados por alguns clientes SSH, como por exemplo, o *openssh*. O funcionamento destes túneis necessita de um servidor de SOCKS residente no cliente SSH. O servidor de SOCKS recebe pedidos das aplicações, que sabem trabalhar com este protocolo, e vai definir túneis de saída baseando-se nos pedidos que forem chegando pelo SOCKS. O protocolo SOCKS cria o túnel de saída definindo o endereço TCP ou UDP a que o cliente pretende aceder. O acesso ao túnel é feito através do servidor SOCKS. A grande limitação deste método é que apenas trabalha com aplicações que saibam "falar" SOCKS.

Para que se possa estabelecer uma ligação segura SSH tem de existir a autenticação do utilizador e a autenticação do serviço de SSH. A autenticação do utilizador pode ser feita usando senhas ou usando um par de chaves assimétricas RSA do utilizador. Por sua vez, o serviço SSH autentica-se por um par de chaves assimétricas DSS ou RSA. Cada serviço SSH pode limitar a exploração dos túneis por parte dos utilizadores.

A grande limitação de uma VPN SSH é o protocolo de transporte, ou seja, o SSH apenas opera com o protocolo TCP. Se fosse necessário usar o protocolo de transporte UDP já não seria possível optar por esta solução.

Uma outra limitação é a necessidade de se definir vários túneis e de se configurar as várias aplicações para que se possa ter vários pedidos a correr no TCP. Evidentemente que os túneis dinâmicos resolveriam estas limitações, mas apenas podemos usá-los em aplicações que trabalhem com SOCKS.

O encapsulamento e a cifra de ligações TCP por SSH são mais uma limitação. Quer isto dizer, que se uma *firewall* está a filtrar pacotes, não actuará porque apenas irá concluir que existe algum tráfego entre a máquina do utilizador e o serviço de SSH. O encapsulamento dos fluxos TCP não permite que a protecção da rede seja feita da melhor forma.

2.4.5.2. VPN SSL/TLS

O TLS (*Transport Layer Security*) e o seu antecessor, SSL (*Secure Sockets Layer*), são protocolos criptográficos que fornecem segurança a comunicações via Internet para serviços, como o *e-mail* (SMTP – *Simple Mail Transfer Protocol*), a navegação por páginas (HTTP – *Hypertext Transfer Protocol*) e também outros tipos de transferência de dados.

Existem algumas pequenas diferenças entre o SSL3.0 e o TLS1.0, mas o protocolo permanece substancialmente o mesmo. O TLS é bastante semelhante ao SSL, mas suficientemente diferente para que haja coexistência dos dois protocolos em diversas aplicações distribuídas.

O modo de funcionamento consiste no seguinte: o servidor que está a ser acedido envia uma chave pública ao *browser* do utilizador, este utiliza-a para a troca de dados encriptados. O transporte de informação segura permite efectuar compressão de dados e garante a confidencialidade e controlo da integridade desses mesmos dados que estão a ser transferidos.

O SSL usa três funções criptográficas. Uma delas prende-se com a necessidade dos dois extremos necessitarem de um meio de transferência de chaves entre si, em que parte deste intercâmbio possibilita a autenticação no servidor. Outra função mostra a obrigatoriedade da existência no protocolo de um método de encriptação de dados da aplicação e de outras mensagens seguras. Por esta razão, o SSL suporta várias cifras, tanto de fluxo como de bloco.

Uma outra função vinca que cada informação transmitida tem de ser autenticada. Para tal, é necessário usar um compilador criptográfico – HMAC (*Hash Message Authentication Code*). Uma das entradas do HMAC é o número sequencial, deste modo, detectam-se ataques por repetição e alterações dos dados.

O SSL suporta uma comunicação segura cliente-servidor sobre a camada de transporte TCP, e é constituído por dois sub-protocolos, o *SSL Handshake Protocol*, que gere a criação e a manutenção de sessões seguras, e o *SSL Transport Protocol*, que controla o transporte seguro sobre um protocolo inseguro (TCP), usando os parâmetros e algoritmos criptográficos associados à sessão.

O HTTPS pode ser definido, genericamente, como HTTP *Secure* sobre uma ligação SSL. No entanto, o SSL pode ser utilizado por outros protocolos da camada de aplicação.

Figura 7 – SSL no modelo TCP/IP.

Analisando o modelo TCP/IP constata-se que o SSL está numa sub-camada localizada entre a camada de aplicação e a camada de transporte.

Por sua vez, o SSL é dividido em duas camadas, a *Handshake Layer* e a *Record Layer*.

Figura 8 – Camadas do SSL.

A sub-camada *Handshake* é dividida em três protocolos: o *Handshake*, que é usado para negociar a sessão cliente-servidor, nomeadamente a troca dos certificados digitais e definição de algoritmos criptográficos que serão usados; o *Change Cipher Spec* que é uma mensagem para notificar o receptor que as próximas mensagens enviadas serão encriptadas com as chaves acabadas de negociar; e o *Alert* que serve para informar que ocorreu um erro ou alguma ocorrência importante, como por exemplo, que a mensagem não pode ser desencriptada ou que a negociação foi rejeitada.

A sub-camada *Record* não é mais do que a encriptação dos dados da camada de aplicação.

2.4.5.3. VPN L2TP

O protocolo L2TP (*Layer 2 Tunneling Protocol*) é um protocolo de *tunneling* que fornece uma VPN de nível 2.

Para as redes IP, o L2TP tramas PPP em datagramas UDP que navegam entre clientes e servidores L2TP. Este protocolo permite o encapsulamento de PPP sobre circuitos virtuais permanentes *Frame relay*, circuitos virtuais X25 e circuitos virtuais ATM.

Este protocolo permite também uma gestão diferenciada da qualidade de serviço, sendo possível estabelecer vários túneis entre o mesmo cliente e o mesmo servidor.

No L2TP fornece autenticação das entidades que realizam o encapsulamento.

A estrutura de uma trama L2TP é mostrada de seguida.

Figura 9 – Trama L2TP.

O MAC *header* é um cabeçalho de nível 2 que depende do meio físico em que está a circular. O IP *header* é um cabeçalho IP que contém os endereços IP da origem e do destino de um túnel L2TP. O UDP *header* contém os portos que estão associados a aplicações de gestão do túnel L2TP. A trama PPP é o que realmente se quer trocar, e que pode conter um datagrama de nível 3 (IP).

Como o L2TP não fornece confidencialidade nem uma autenticação poderosa, recorre-se ao IPSec para que os pacotes L2TP sejam providos de confidencialidade e integridade.

Para que se possa estabelecer um canal seguro, há uma negociação de IPSec SA (*Security Association*) através do IKE (*Internet Key Exchange*), seguida da criação de uma comunicação ESP (*Encapsulating Security Payload)* em modo de transporte. Finalmente, há uma negociação e é estabelecido um túnel seguro L2TP entre as extremidades SA com encriptação IPSec. Depois deste processo, os pacotes L2TP, que estão entre as extremidades do túnel, são encapsulados pelo IPSec.

No protocolo L2TP há uma separação entre os serviços de encapsulamento de tráfego e os serviços de segurança fornecidos pelo IPSec. Os serviços de segurança operam em todas as trocas de dados e garantem autenticidade.

2.4.5.4. VPN PPTP

O PPTP (*Point-to-Point Tunneling Protocol*) é um protocolo que resultou da modificação do PPP (*Point-to-Point Protocol*), com muitos aspectos semelhantes ao L2TP, mas diferenciado na forma de encapsular.

O PPP é um protocolo capaz de ligar duas máquinas através de uma única conexão física. É um protocolo que ficou popularizado na Internet por ligar máquinas e redes a routers de acesso à Internet através de conexões *dial-up*. É um protocolo de nível 2 (ligação de dados), que actua física e logicamente.

Uma outra modificação do PPP é o PPPoE (*Point-to-Point over Ethernet*). O PPPoE é um protocolo que através de uma rede *Ethernet* interligar diversas máquinas.

O PPP utiliza o ECP (*Encryption Control Protocol*) para cifrar os dados na ligação, mas não possui nenhum mecanismo que verifique a sua integridade. Como não há forma de verificação dos dados, não existe correcção de dados, quer na origem, quer no destino.

O ECP não utiliza chaves de sessão durante a autenticação, visto que o PPP não disponibiliza essa funcionalidade, sendo uma outra limitação deste protocolo.

O PPP dispõe de dois protocolos de autenticação: PAP (*Password Authentication Protocol*) e CHAP (*Challenge Handshake Authentication Protocol*), em que é autenticada a origem quando o utilizador inicia a ligação.

Em suma, o PPP é um protocolo que não satisfaz os requisitos mínimos de uma VPN, pelo facto de não garantir segurança suficiente e pela necessidade de um único meio físico para cada ligação. Usando o PPP numa VPN necessitar-se-ia de uma ligação física entre a origem e o destino, levando a um aumento de custos.

Para corrigir as limitações do PPP, surge o PPTP. O PPTP é um protocolo que permite uma ligação PPP entre dois pontos extremos que saibam comunicar via IP. Foi criado e desenvolvido pela Microsoft.

A grande vantagem do PPTP, comparativamente com o PPP, é termos um túnel sobre IP onde são trocadas tramas PPP entre os dois pontos extremos, por exemplo, entre uma máquina do cliente e um router que dê acesso a uma LAN ou à Internet.

Se um utilizador estiver ligado a uma LAN ou a um ISP e a um servidor de acesso PPTP (PPTP RAS – PPTP *Remote Access Server*), então o túnel PPTP permite que haja uma ligação segura através da Internet.

Uma ligação PPTP, acrescida de segurança, permite que seja criada uma VPN ao nível da ligação de dados (nível 2). Uma das vantagens deste tipo de VPN é conseguir que uma máquina remota (utilizador) trabalhe como se estivesse fisicamente ligada à rede que acedeu via VPN. Isto traduz-se nas tramas trocadas, ou seja, as tramas não necessitam de ser encapsuladas em IP. Esta vantagem pode tornar-se numa desvantagem se a ligação for de baixo débito, em que haverá uma sobrecarga de tráfego desnecessário.

O PPTP garante a autenticação da origem e do destino e disponibiliza as chaves de sessão. Com o uso das chaves de sessão, os dados em trânsito numa ligação podem ser cifrados recorrendo ao MPPE (*Microsoft Point-to-Point Encryption*). Só é possível considerar uma VPN PPTP quando é usado o protocolo MPPE.

Apesar do PPTP permitir a cifra do tráfego PPP, esta cifra só é aplicada depois da autenticação ser concluída. Quer isto dizer, que não há segurança na autenticação.

Os protocolos de autenticação PAP e CHAP são usados em PPTP, assim como algumas extensões do EAP (*Extended Authentication Protocol*). Numa VPN PPTP, estes dois protocolos de autenticação (PAP e CHAP) não devem ser usados porque não activam a cifra da ligação PPTP. O protocolo de autenticação usado numa VPN PPTP é o MS-CHAPv2. No entanto podem também ser utilizadas extensões do EAP. O MS-CHAPv2 permite autenticar os dois pontos extremos do túnel simultaneamente, recorrendo à partilha da senha e das respostas trocadas.

O PPTP permite a autenticação das entidades que dialogam por PPP, enquanto que o L2TP permite a autenticação das entidades responsáveis pelo encapsulamento.

O protocolo de cifra de dados usado numa VPN PPTP é o MPPE, como já foi referido. Este protocolo usa chaves simétricas de três tamanhos possíveis, e duas chaves diferentes por cada ligação (uma em cada sentido).

Uma das limitações do MPPE é a ausência de verificação da integridade dos dados recebidos usando mecanismos criptográficos, garantindo apenas a confidencialidade dos dados úteis trocados pelo tráfego PPP encapsulado.

O PPTP é eficiente em encapsular o tráfego PPP através da Internet, o que possibilita a um utilizador remoto o acesso a uma rede com um servidor PPTP. Mas as suas limitações prendem-se com a falta de segurança de base e com a necessidade da configuração do protocolo de autenticação.

Uma VPN PPTP é de fácil configuração e utilização, mas não será aconselhável quando a segurança é um factor crítico.

2.4.5.5. VPN IPSec

O IPSec (*IP Security*) trata-se da tecnologia *standard* do IETF, opera na camada de rede (modelo OSI) e é indiferente ao tipo de tráfego que transporta. Desta forma é transparente para as aplicações.

O capítulo seguinte será alvo do seu estudo.

2.4.6. IPSec

Uma das características essenciais e desejáveis quando se trabalha com o IPSec é a variedade de diferentes parâmetros e configurações possíveis, para conseguir com sucesso uma ligação VPN IPSec.

Uma das causas da complexidade do IPSec é o vasto leque de mecanismos e conjuntos de ferramentas que é fornecido, permitindo uma qualquer implementação em que os extremos da ligação acabam por pactuar.

2.4.6.1. AH vs.ESP

O AH (*Authentication Header*) e o ESP (*Encapsulating Security Payload*) são os dois principais protocolos usados pelo IPSec, pois o AH autentica e o ESP encripta ao mesmo tempo que autentica os dados transferidos através de uma ligação.

Estes protocolos são usados de forma independente, contudo é possível operá-los em conjunto, não sendo muito comum.

O AH é usado para autenticar, não encriptar, o tráfego IP, servindo o propósito de assegurar que se está realmente a dialogar apenas com quem se pretende. É usado, também, para a detecção de alteração de dados enquanto estão a ser transferidos, e (opcionalmente) para proteger contra ataques de reinserção de dados capturados anteriormente.

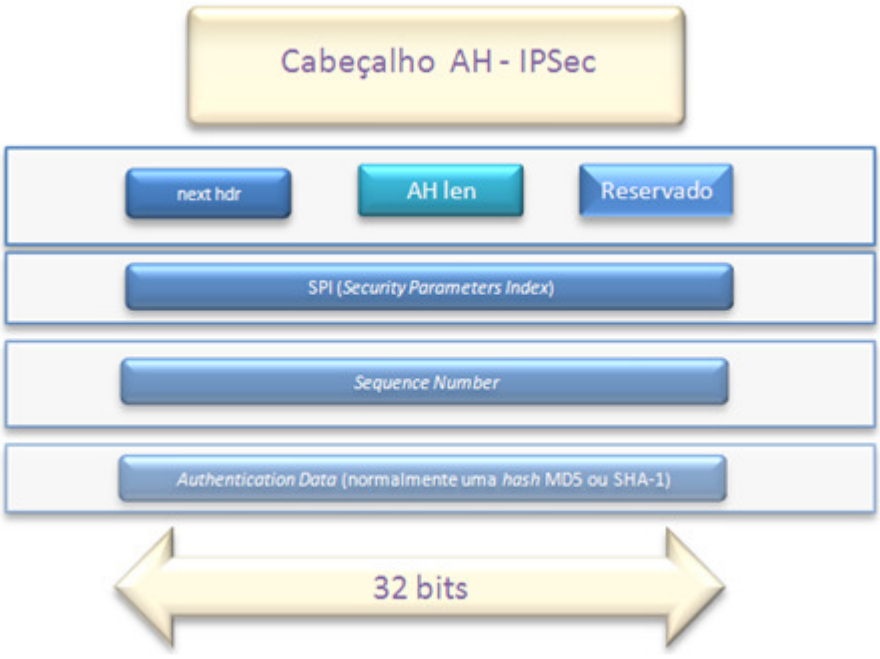


Figura 10 – Cabeçalho AH do IPSec.

A autenticação é feita pela avaliação de uma *hash* criptográfica baseada no código da autenticação da mensagem em quase todos os campos do pacote IP, guardando-a nos cabeçalhos AH recentemente adicionados.

O cabeçalho AH contém apenas cinco campos de interesse, e é injectado entre o cabeçalho IP original e os dados transferidos.

A figura da página anterior esboça o formato do cabeçalho do AH. O *next hdr* identifica o tipo de protocolo tornando possível a ligação entre cabeçalhos IPSec. O AH *len* define o tamanho do cabeçalho AH. O SPI é um identificador que ajuda o receptor a identificar a qual das várias ligações este pacote se aplica. O *Sequence Number* não é mais que um contador crescente que protege contra ataques de reinserção. O *Authentication Data* é o ICV (*Integrity Check Value*) calculado sobre todo o pacote IP, incluindo os cabeçalhos, onde valores errados marcam o pacote como corrompidos e de seguida descartados.

2.4.6.2. Modo Túnel vs. Modo Transporte

O modo de transporte fornece uma ligação segura entre dois extremos, na qual encapsula os dados IP. O modo túnel encapsula todo o pacote IP de modo a criar uma ligação virtual segura entre as duas *gateways*. O modo túnel é usado para formar a VPN tradicional, criando um túnel seguro através da Internet.

O modo de transporte é usado para proteger uma comunicação entre dois extremos. Esta protecção é fornecida pela autenticação ou pela encriptação, ou ambas. Contudo, não é um protocolo relacionado com túneis, nem sequer se relaciona com uma VPN tradicional, é simplesmente uma conexão IP segura.

No AH no modo de transporte, o pacote IP é ligeiramente alterado incluindo um novo cabeçalho AH entre o cabeçalho IP e os dados transferidos no protocolo. Há também uma troca do código de protocolo ligando assim os vários cabeçalhos, e permitindo que o pacote IP original possa ser reconstituído no destino. Após os cabeçalhos IPSec serem validados na recepção, os mesmos são retirados e o tipo de protocolo original (TCP, UDP, …) é colocado novamente no cabeçalho IP.

O modo túnel forma a mais familiar funcionalidade de uma VPN, onde todos os pacotes IP são encapsulados dentro de outro e entregues no seu destino.

No modo de transporte, o pacote é selado com uma verificação de integridade ICV para autenticar o remetente e para impedir a sua modificação na transferência. Mas ao contrário do modo de transporte, o modo túnel encapsula totalmente o cabeçalho IP, bem como os dados (*payload*), permitindo que os endereços de origem e destino sejam diferentes do endereço do pacote abrangente, dando origem a um túnel.

Quando o pacote chega ao seu destino, este passa a verificação de autenticação como qualquer outro pacote do tipo AH, e aqueles que passam a verificação têm todo o seu cabeçalho IP e AH retirados. Este processo reconstitui o pacote IP no original.

A maioria das implementações, no modo túnel, trata a extremidade da conexão como um interface virtual de rede, tal como uma interface *Ethernet*, sendo o tráfego de entrada ou saída sujeito às decisões de *routing* em causa.

O pacote reconstituído pode ser entregue à máquina local ou encaminhado, de acordo com o endereço IP de destino inserido no pacote encapsulado, embora neste caso não continue sujeito à protecção do IPsec, pois nesta fase é apenas um pacote IP normal.

Embora o modo de transporte seja utilizado estritamente para garantir a segurança de uma conexão entre extremos numa comunicação entre duas máquinas, o modo túnel fornece uma VPN, sendo usado tipicamente entre as *gateways* de uma rede (routers, *firewalls* ou dispositivos autónomos de VPN).

2.4.6.3. Criptografia

Configurar uma VPN IPSec pode envolver todos os tipos de opções de criptografia, mas esta é substancialmente simplificada pelo facto de que uma ligação pode usar dois ou três tipos de cada vez, sendo mais comum optar por dois tipos.

A autenticação calcula um ICV sobre o conteúdo do pacote de dados, e é geralmente construída em cima de uma *hash* criptográfica, sequência de bits, como o MD5 ou SHA-1. Esta incorpora uma chave secreta conhecida de ambos os lados, permitindo que o destinatário calcule o ICV da mesma forma. Se o destinatário receber o mesmo valor, o remetente encontra-se efectivamente autenticado. O AH fornece sempre autenticação, enquanto o ESP tem-na como opcional.

A criptografia, também designada por vezes encriptação, usa uma chave secreta para encriptar os dados antes da transmissão, o que esconde o real conteúdo do pacote de curiosos. Os algoritmos criptográficos disponíveis para este caso são principalmente o DES, 3DES, *Blowfish* e AES, podendo serem usados outros.

Uma vez que ambos os lados da conversação necessitam saber quais os valores secretos utilizados na *hash* ou na encriptação, existe a questão de como esses dados são trocados. As chaves manuais exigem entrada manual dos valores secretos em ambas as extremidades, contudo o IKE é um mecanismo sofisticado que permite efectuar esse processo *on-line*.

Existem dois modos de controlar a eficiência e a segurança durante a troca de chave IKE inicial. O modo principal, requer seis pacotes de ida e volta, oferecendo uma completa segurança durante o estabelecimento de uma ligação IPSec, enquanto o modo agressivo usa metade das trocas proporcionando uma segurança menor, porque algumas informações são transmitidas em texto (*cleartext*).

Capítulo 3

Estado da Arte

Hoje em dia, na aldeia global em que vivemos, cada vez é mais frequente as empresas e os fabricantes de todo o mundo se unirem, criando organizações para uma maior cooperação.

O mercado da tecnologia VPN não é diferente, e deste modo em 1999 foi fundada a VPNC (*Virtual Private Network Consortium*).

Este organismo tem como finalidade promover novos produtos à imprensa e a potenciais clientes, aumentar a colaboração entre membros e manter um fórum de discussão e divulgação de novas soluções tecnológicas. Contudo o VPNC não cria *standards* na tecnologia que representa, mas sim apoia fortemente os *standards* actuais e futuros do IETF.

O mercado das VPNs SSL e IPSec continua a prosperar. Ao mesmo tempo que a importante vertente da tecnologia IPv6 continua em franca expansão neste campo, sendo assinados acordos de interoperabilidade entre fabricantes, tais como a Juniper e a SafeNet.

Uma outra recente vaga nesta tecnologia das VPNs é o seu uso nas comunicações móveis. As *mobile* VPN, designadas por mVPN, são usadas em ambientes onde os utilizadores estão em constantes deslocações, quer num edifício, num *campus* ou no terreno. Estes utilizadores estão permanentemente ligados à rede através de diferentes meios, tais como redes *wireless* ou GSM. Uma VPN convencional não garante este tipo de cenário pois o túnel ao ser desligado provoca a quebra do funcionamento das aplicações. As mVPNs são usadas em hospitais, segurança e serviços externos.

Os grandes fabricantes, tal como é descrito neste capítulo, apostam cada vez mais nesta tecnologia. Os fabricantes, tais como a Cisco, a Juniper, a Check Point, a Citrix, a Fortinet, a D-Link, agregam nos seus produtos todas as potencialidades das VPNs e das *firewalls*, protegendo os seus clientes da Internet, que se torna cada vez mais vulnerável.

A diversidade dos modelos apresentados de seguida exemplifica a grande variedade das soluções existentes no mercado, servindo de base para o estudo da redundância de uma VPN num cenário real.

3.1. A Solução da Check Point - IPSec VPN *Software Blade* – Módulo de *Software* de uma VPN

Esta camada de *software* de VPN da Check Point é uma solução de *software* integrada que fornece conectividade segura para redes corporativas, utilizadores remotos e móveis, sucursais e parceiros de negócio.

O módulo integra controlo de acessos, autenticação e encriptação, e garante segurança nas conexões de rede na passagem pela Internet.

Esta solução é simples, tem gestão centralizada do acesso remoto e dos vários pontos em que a VPN é acedida. Este *software* permite um nível de segurança elevado da VPN IPSec. Um outro benefício é a possibilidade de existirem múltiplos modos de acesso remoto de conectividade VPN para suportar as várias adversidades que surjam no caminho a todas as localizações e redes.

As especificações deste *software* são:

Característica	Detalhe
Métodos de autenticação	Palavra-chave, RADIUS, TACACS, X.509, SecurID
Certificado de autorização	Certificado de autorização integrado X.509
Comunidades VPN	Configura automaticamente ligações *site* a *site* à medida que os objectos são criados
Suporte à topologia	Estrela e *mesh*
VPN baseada em *routing*	Utiliza túneis de interfaces virtuais
Injecção de rotas na VPN	Mecanismo de injecção de rotas (RIM)
Modos de VPN *site* a *site*	Baseados em domínios, baseados em rotas
VPN direccional	Execução entre e dentro do comunidade
Troca de chaves IKE (Fase 1)	AES-256, 3DES, DES, CAST
Integridade de dados IKE (Fase 1)	MD5, SHA1
Encriptação de dados IPSec (Fase 2)	3DES, AES-128, AES-256, DES, CAST, DES-40CP, CAST-40, NULL
Integridade de dados IPSec (Fase 2)	MD5, SHA1
Grupos *Diffie-Hellman* IKE (Fase 1) e IPSec (Fase 2)	Grupo 1 (768 *bit*), Grupo 2 (1024 *bit*), Grupo 5 (1536 *bit*), Grupo 14 (2048 *bit*)
Opções IKE (Fase 1)	*Aggressive Mode*
Opções IPSec (Fase 2)	*Perfect Forward Secrecy,* compressão IP
Suporte a dispositivos móveis	Suporte de L2TP no iPhone, *SecureClient Modile* para o *Windows Mobile*
Clientes de VPN IPSec variados	*Check Point Endpoint Security, SecureClient, SecuRemote*

Tabela 1 – Especificações do *software* da Check Point.

Esta solução tem várias características importantes: uma simples implementação de VPN *site-to-site*, vários métodos de criação de VPN, uma elevada segurança numa VPN IPSec, um suporte de acesso remoto flexível e vários modos de conectividade VPN de acesso remoto.

O módulo de *software* IPSec fornece um método único para criar e gerir VPNs complexas. A *SmartDashboard* permite que os gestores de rede definam as *gateways* que integram a VPN. As *gateways* da VPN podem ser configuradas para as topologias em estrela e emalhada para gestão de chaves.

Este *software* permite vários métodos de criação de VPNs. As VPNs podem ser baseadas em rotas, em que é definido que tráfego é que deve ser encriptado pelo método escolhido, permitindo a criação de uma VPN complexa e de grande escala em ambientes dinâmicos. As VPNs baseadas em rotas também suportam a extensão do *routing* dinâmico e do *multicast* através delas próprias. As VPNs podem ser ainda baseadas no domínio, em que são definidos quais os recursos que devem encriptar o tráfego da VPN através da *gateway*.

Uma outra característica é a elevada segurança numa VPN IPSec. Um elemento chave da filosofia da Check Point é que a conectividade VPN tem de ser combinada com um elevado grau de segurança. O módulo de *software* IPSec permite conecta utilizadores remotos, locais e parceiros sem que haja a preocupação da VPN se tornar uma rede secreta. Este *software* pode aplicar a política de segurança total ao tráfego encriptado, a um pedaço de tráfego, ou permite que o tráfego da VPN seja desconhecido. Para além de tudo isto, existe ainda um mecanismo IKE que fornece uma elevada segurança para as VPNs contra os ataques DoS (*Denial of Service*). O módulo IPSec implementa uma solução única para IKE DoS, perguntando quais as *gateways* desconhecidas que se tem de conectar para resolver um problema computacional intenso (grave), antes da alocação de recursos.

Como cada empresa tem as suas exigências para o acesso remoto, é aconselhável que o suporte de acesso remoto seja flexível. Este *software* fornece flexibilidade para desenhar uma solução que vá de encontro às necessidades do cliente da VPN de acesso remoto.

O módulo de IPSec fornece vários modos para endereçar as várias formas de conectividade e de encaminhamento, que surgem para os utilizadores remotos. O modo "*Office Mode*" faz a atribuição do *routing* entre o cliente e a *gateway* pelo encapsulamento dos pacotes IP com os endereços IP originais dos utilizadores remotos, permitindo que os utilizadores apareçam como se estivessem no *office* quando estão conectados remotamente. Este modo também fornece o *anti-spoofing*, assegurando que o endereço IP que foi encontrado pela *gateway* é autêntico e atribuído ao utilizador. O modo "*Visitor Mode*" permite que os colaboradores acedam aos recursos enquanto estejam a trabalhar numa localização remota, tal como um hotel ou um escritório de um cliente, onde a Internet pode ser limitada pela *Web Browsing* usando os portos de HTTP e HTTPS. O modo "*Hub Mode*" permite rigor, controlo centralizado do tráfego de todos os clientes, removendo a necessidade de funções de segurança nos vários escritórios, e dando comunicações seguras *client-to-client*, tal como VoIP ou conferências pela Internet usando aplicações como o "*Microsoft NetMeeting"*.

Como as ameaças à rede são cada vez mais frequentes e tornam-se cada vez mais sofisticadas, a Check Point desenvolveu este *software* com mecanismos de protecção a este tipo de ameaças. Os benefícios desta camada de *software* prendem-se com a segurança contínua aos pontos de acesso mais críticos e aos pacotes de serviço.

3.2. A Solução da Juniper

A Juniper Networks possui componentes integrados capazes de combater o grande problema de segurança de uma rede, optimizando o desempenho dos equipamentos. Os componentes foram desenhados para contribuir para uma rede robusta e segura.

Com plataformas de capacidade elevada e segurança integrada e com o *routing* LAN/WAN através de interfaces físicos de rede (LAN/WAN), os componentes da Juniper Networks integram dispositivos de segurança como *SSG, ISG*, *NetScreen* e os produtos *SRX* focam as necessidades das empresas do sector público. Estes dispositivos podem proteger a rede de muitos ataques e facilita as comunicações de negócio seguras.

A Juniper Networks tem vários segmentos de produtos, como por exemplo, serviços de *Auto Connect VPN* e *de Dynamic VPN*, que ajudam a diminuir a carga administrativa associada com as distribuições de IPSec.

Para que haja protecção dos ataques ao nível da rede, os equipamentos Juniper Networks usam um método dinâmico de filtragem de pacotes. Com este método, as *firewalls* agregam informação dos vários componentes no cabeçalho do pacote, incluindo os endereços IP da origem e do destino, os números dos portos de origem e de destino e as sequências de números dos pacotes. Quando chega um pacote de resposta, a *firewall* compara a informação que vem no cabeçalho com a informação que tem associada. Se não corresponder, então o pacote é descartado.

Por defeito, a *firewall* da Juniper nega todo o tráfego em todas as direcções.

A conectividade WAN segura, desempenha um papel importante na protecção do nível de rede. Desenvolvendo redes privadas virtuais (VPNs) robustas, os locais remotos podem ser conectados de forma segura a outros locais remotos, e podem centralizar os dados e as aplicações usando a Internet como meio físico. Características como *Auto Connect VPN*, disponível em alguns modelos, pode ajudar e facilitar a administração e a gestão das VPNs.

Para ajudar a bloquear ataques nefastos ao nível das aplicações, a Juniper Networks integra a prevenção da intrusão através de uma linha de produtos. Para locais centrais da empresa, para ambientes do centro de dados e para as redes de fornecedores de serviços com elevado volume de produção, a Juniper Networks tem uma linha de grande desempenho: SRX100, SRX210, SRX240, SRX650, SRX3000 e SRX5000.

Figura 11 – Equipamento da Juniper.

Para escritórios remotos ou pequenas localizações sem pessoas a tempo inteiro, a integração e a simplicidade é fundamental numa solução segura. Normalmente, a Juniper Networks fornece protecção integrada de antivírus baseado em ficheiros da *Kaspersky*, nos equipamentos Juniper Networks SSG e SRX. Estes produtos combinam as capacidades de *firewall* e de VPN com antivírus bastante desenvolvido. Este antivírus opera no tráfego da *Web* e no *e-mail*, examinando os protocolos IMAP, SMTP, FTP, POP3, HTTP.

As tecnologias virtuais na VPN da Juniper Networks e as soluções de segurança do router permitem aos utilizadores segmentar a rede em vários pedaços, controlando tudo num único dispositivo. Os gestores da rede podem segmentar o tráfego para destinos diferentes ou podem dividir a rede em segmentos distintos, com o uso de *firewall* ou políticas de segurança separada.

Estes dispositivos VPN suportam tecnologias como as zonas seguras, os sistemas virtuais, os routers virtuais e as VLANs.

As zonas seguras representam as secções virtuais da rede, segmentadas em áreas lógicas, podendo ser atribuídas a uma interface física ou a um sistema virtual. Quando as zonas seguras são atribuídas a um sistema virtual, muitas zonas podem partilhar uma única interface física, diminuindo os custos.

Os sistemas virtuais (*Virtual Systems* - VSYS) são um nível adicional de partição que cria múltiplos ambientes virtuais independentes, cada um com os seus utilizadores, *firewalls*, VPNs, políticas de segurança e interfaces de gestão. Se os gestores da rede segmentarem a rede em múltiplos ambientes seguros controlados através de um único dispositivo, VSYS permite sejam construídas soluções de múltiplos clientes em poucas interfaces físicas. Esta redução traduz-se em capital e em operacionais.

Os Routers Virtuais (*Virtual Routers* – VR) permitem dividir um único equipamento em funções como se existissem múltiplos routers físicos. Cada router virtual pode suportar os seus próprios domínios, assegurando-se que nenhuma informação de *routing* é passada para os domínios dos outros routers virtuais. Isto traduz-se na vantagem de um simples equipamento suportar múltiplos ambientes de cliente, diminuindo o custo.

As *Virtual* LANs (VLAN) são divisões lógicas de rede que permitem aos gestores de rede identificarem e segmentarem o tráfego em vários níveis. As políticas de segurança podem definir como o tráfego é encaminhado da cada VLAN para um zona segura, um sistema virtual ou uma interface física. Esta característica permite uma maior facilidade de identificar e organizar o tráfego de vários departamentos, definindo quais os recursos que cada um pode aceder.

Como é possível verificar no esquema da figura seguinte, o uso da tecnologia virtual permite segmentar uma rede em hierarquias de seguros compartimentos:

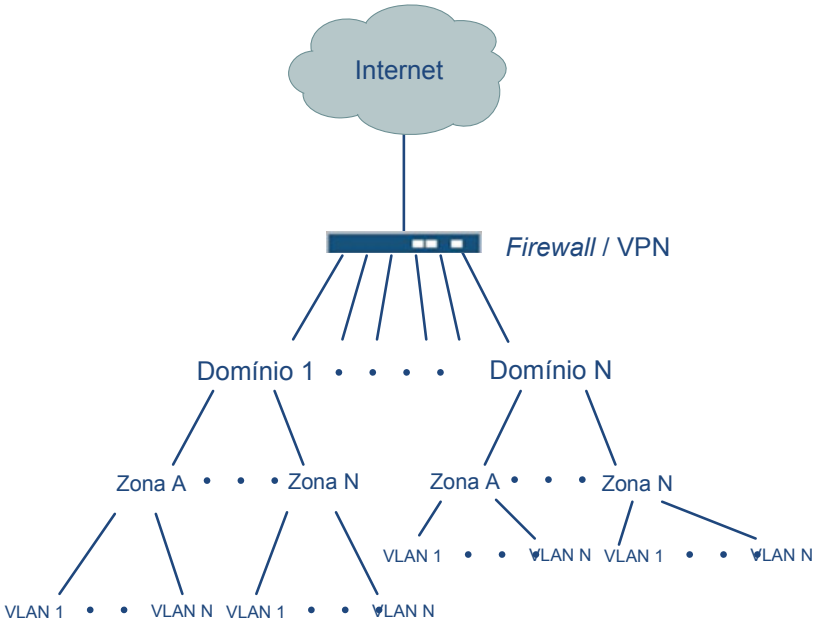


Figura 12 – Exemplo da Segmentação de uma rede recorrendo ao equipamento da Juniper.

A Juniper Networks garante soluções que incluem sistemas de confiança e de alto desempenho baseadas no protocolo NSRP (*NetScreen Redundancy Protocol*) e no JSRP (*Juniper Services Redundancy Protocol*). As *firewalls* e as VPNs podem ser garantidas pelo serviço de redundância com ajuda de um dispositivo de recurso. A configuração pode ser feita da seguinte forma:

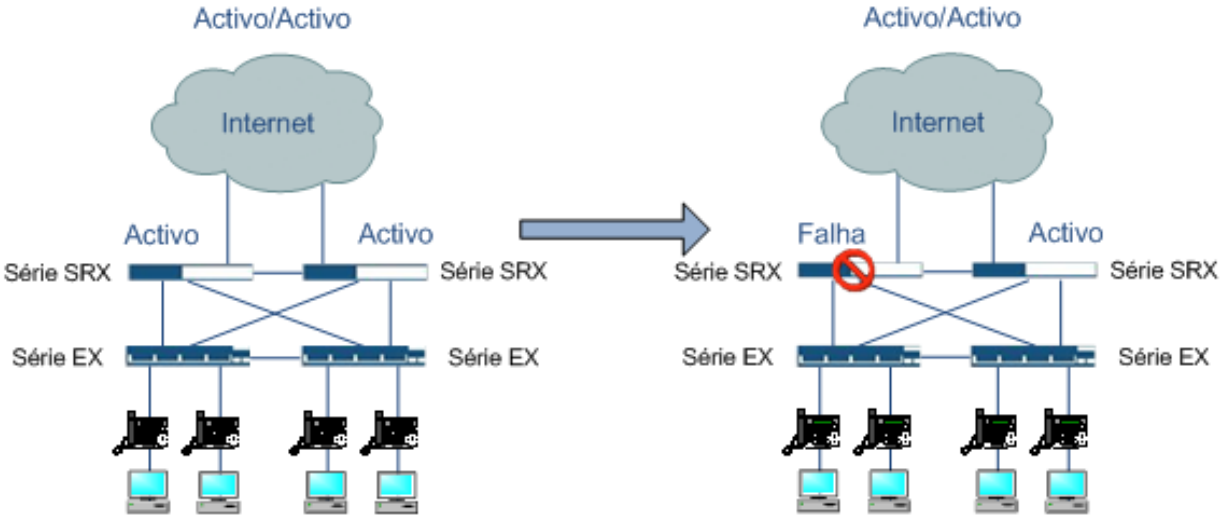


Figura 13 – Configuração de uma VPN e/ou *firewall* com redundância activo/activo.

Há duas formas de configurar esta redundância: activo/passivo e activo/activo.

No activo/passivo, o dispositivo principal partilha toda a rede, todas as configurações e toda a informação de sessão actual com um dispositivo de reserva (*backup*). Assim, no caso de falha, o dispositivo de reserva pode desempenhar as funções do dispositivo principal sem qualquer problema. A rede da Juniper Networks e a gestão de segurança fornecem o controle centralizado e baseado nas políticas de segurança.

No activo/activo, ambos os dispositivos são configurados para serem os principais, com tráfego a passar por cada um. Se um dispositivo falhar, o outro dispositivo assume-se como principal e continua com todo o tráfego. A redundância física fornece uma maior robustez e um melhor tempo de resposta.

Como as redes nunca são estáticas, e como as mudanças têm custos e demoram tempo, este fabricante propõe três modos de funcionamento.

O modo transparente recorre à maneira mais simples de dar segurança a uma rede. As organizações podem desenvolver um dispositivo de VPN Juniper Networks sem fazer nenhuma alteração na rede. As funções da VPN fazem-se sem um endereço IP, tornando o equipamento invisível ao utilizador.

O modo *route* permite ao dispositivo de segurança participar activamente no *routing* da rede, suportando protocolos de *routing* estático e dinâmico, incluindo BGP, OSPF, RIPv1, RIPv2 e ECMP. Este modo garante aos gestores da rede a facilidade e rapidez de soluções de segurança de várias camadas com uma configuração manual mínima.

O modo NAT converte automaticamente um endereço IP ou um grupo de endereços IP num único endereço, para esconder endereços confidenciais de uma organização de serem vistos por todos.

As soluções da Juniper Networks suportam endereçamento, tanto estático como dinâmico, com DHCP e PPPoE, permitindo que os dispositivos operem em qualquer ambiente de rede.

A Juniper Networks fornece uma plataforma de gestão, *Network and Security Manager.* Esta plataforma permite a um gestor de rede controlar as especificações da sua VPN/*firewall*, incluindo a configuração, os parâmetros de rede e as políticas de segurança.

3.3. A Solução da Cisco

A Cisco aconselha, para garantir protecção, que todas as redes devem incluir componentes de segurança em cinco áreas críticas: identidade, segurança da periferia, ligação segura, monitorização de segurança e gestão da política de segurança.

A solução para a identidade centra-se no servidor Cisco *Secure Access Control Server*.

Na segurança da periferia oferecem uma vasta gama de escolhas de *firewall* baseadas na Cisco *Secure PIX firewall*, na Cisco ASA *firewall* ou no IOS *firewall*.

Uma ligação segura pode ser estabelecida utilizando VPNs que podem ser divididas em *Remote Access* VPNs (RPVs *site-to-site* e RPVs de acesso remoto). As *Site-to-Site* VPNs são idealmente construídas com routers optimizados para VPNs, os Cisco 800, 1700, 2600, 3600, 7100 e 7200.

Para resolver a questão da monitorização da segurança existe o Cisco *Secure* IDS e o Cisco *Secure Scanner*, que são ferramentas que diminuem a vulnerabilidade da rede.

Finalmente, a gestão da política de segurança pode ser efectuada utilizando o Cisco *Secure Policy Manager*.

Os produtos PIX *firewall*, ASA *firewall*, Cisco *Secure* IDS e Cisco VPN tornaram-se rapidamente nos líderes de mercado no segmento da segurança. O futuro do PIX e do ASA é muito promissor. O IDC (*International Data Corporation*) prevê que o mercado para as *firewalls* baseadas em hardware cresça ao dobro do ritmo do mercado para as *firewalls* baseados em *software*.

As principais soluções apresentadas pela Cisco referentes a este segmento são expostas de seguida.

3.3.1. Cisco ASA 5500 *Series* SSL/IPSec VPN *Edition*

Este equipamento fornece, de uma forma segura e flexível, o acesso remoto à rede de qualquer parte.

O Cisco ASA 5500 *Series* SSL / IPSec VPN *Edition*, também conhecida como a solução Cisco *Secure Remote Access*, abrange um conjunto de funcionalidades de SSL, de VPN IPSec, de *firewall,* de IPS (*Intrusion Prevention System*) e de tecnologias de segurança de conteúdo numa única plataforma, escalável e de elevado desempenho.

Para o acesso sem restrições à rede, assim como o acesso controlado a aplicativos baseados na *Web* e recursos de rede, o Cisco *Secure Remote Access* disponibiliza a flexibilidade necessária para qualquer solução de VPN, como se pode perceber no esquema da figura catorze.

A solução é de fácil implementação e simples de usar, oferecendo tanto a opção *client* como a *clientless*. Esta aplicação resolve os problemas associados com grupos de utilizadores e terminais diversos que acedam à rede da empresa, oferecendo um controlo de acesso escalável, dependendo do utilizador ou do equipamento terminal, mantendo a integridade das informações confidenciais.

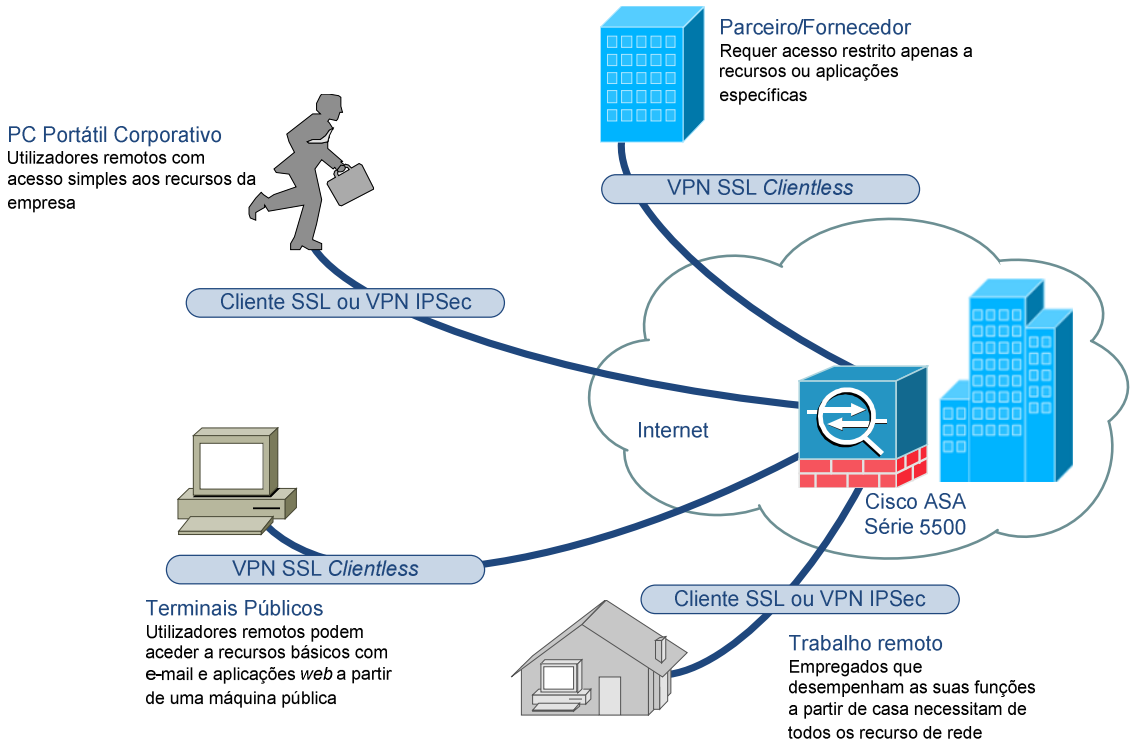


Figura 14 – Serviço VPN SSL e IPSec optimizado para vários cenários de implementação.

Um dos benefícios destes equipamentos é a implementação flexível, onde se estende a tecnologia SSL VPN, quer a utilizadores *clientless* ou com acesso total à rede, dependendo do grupo de utilizadores ou terminal.

O acesso à rede é abrangente, ou seja, as aplicações e os recursos de rede são fornecidos através do *AnyConnect* Cisco VPN *Client*, um cliente (*plugin*) descarregado automaticamente que cria o túnel seguro para a rede.

Mais uma característica destes equipamentos é o desempenho optimizado da rede. Isto é, o Cisco *AnyConnect* VPN *Client* disponibiliza uma ligação VPN optimizada para o tráfego sensível a latências, tal como a voz sobre IP (VoIP) ou o acesso a aplicações baseadas em TCP.

A combinação de tecnologias apresenta-se como mais uma vantagem. Para além dos recursos disponíveis através da VPN SSL, os utilizadores também podem usufruir das vantagens da tecnologia VPN IPSec, numa única plataforma. O *Cisco Secure Remote Access* oferece uma solução altamente personalizável para diversos cenários de implementação de VPNs, eliminando o custo da implementação de soluções paralelas de acesso remoto.

Figura 15 – Alguns modelos de equipamentos da Cisco.

Esta solução Cisco apresenta uma ampla gama de modelos disponíveis. As plataformas apresentadas pelo fabricante Cisco estão disponíveis para todos os segmentos de mercado, dependendo das características necessárias para cada solução.

As características fundamentais na fase do projecto de implementação são a largura de banda (*throughput*) máxima para a VPN de 100 Mbit/s até 1 Gbit/s, o número máximo de sessões VPN SSL e/ou VPN IPSec de 25 a 10000 e a capacidade de balanceamento e redundância de tráfego (apenas disponível em alguns modelos).

3.3.2. IPSec VPN *Shared Port Adapter*

Figura 16 – IPSec VPN *Shared Port Adapter*

O Cisco IPSec VPN *Shared Port Adapter* (SPA) é um módulo de alta velocidade IPSec para os routers Cisco da série 7600 e para o switch *Catalyst* da série 6500, fornecendo o serviço de VPN IPSec à infra-estrutura nele integrada, de modo a garantir uma maior fiabilidade e uma maior exigência de largura de banda. Ou seja, se estas plataformas estiverem munidas de módulos de interfaces de rede ligados directamente aos servidores aplicacionais, existem muito menos pontos de falha na rede quando um utilizador remoto acede a estes recursos.

Cada *slot* dos Cisco 7600 e 6500 pode suportar duas SPAs, e apesar destes módulos não possuírem interfaces de rede, tiram partido da largura de banda, LAN e/ou WAN, dos interfaces de cada uma das plataformas.

Uma das características principais desta placa é a sua integração com a infra-estrutura de rede. Ou seja, pode incorporar-se a tecnologia VPN ao *Switch Catalyst* 6500 e ao router 7600, sem a necessidade de mais equipamentos ou de alterações na rede.

O alto desempenho e a escalabilidade são outras características desta placa. Incorporando o mais recente em tecnologia de criptografia de aceleração por hardware, o IPSec VPN SPA pode fornecer até 2,5 Gbit/s de tráfego *Advanced Encryption Standard* (AES) e terminar até 8000 túneis IPSec, simultaneamente, com tempos de execução muito baixos.

Este módulo pode suportar serviços de segurança avançada, que permitem simplificar a implementação segura de um *campus*, a prestação de serviços, a terminação de VPNs e os serviços de rede convergentes, tais como VoIP e redes de armazenamento, através da integração de criptografia, autenticação e integridade aos serviços de rede.

3.3.3. Cisco IOS IPSec

Os dois produtos anteriores representam as melhores soluções da Cisco para a necessidade de uma VPN. Contudo o *portfolio* Cisco apresentado na figura 17 disponibiliza VPNs de acordo com um *software* específico, o Cisco IOS *Advanced Security*. Este *software* combina várias opções de VPN, *firewall* avançado, prevenção à intrusão, QoS, multi-protocolar e opções avançadas de *routing*.

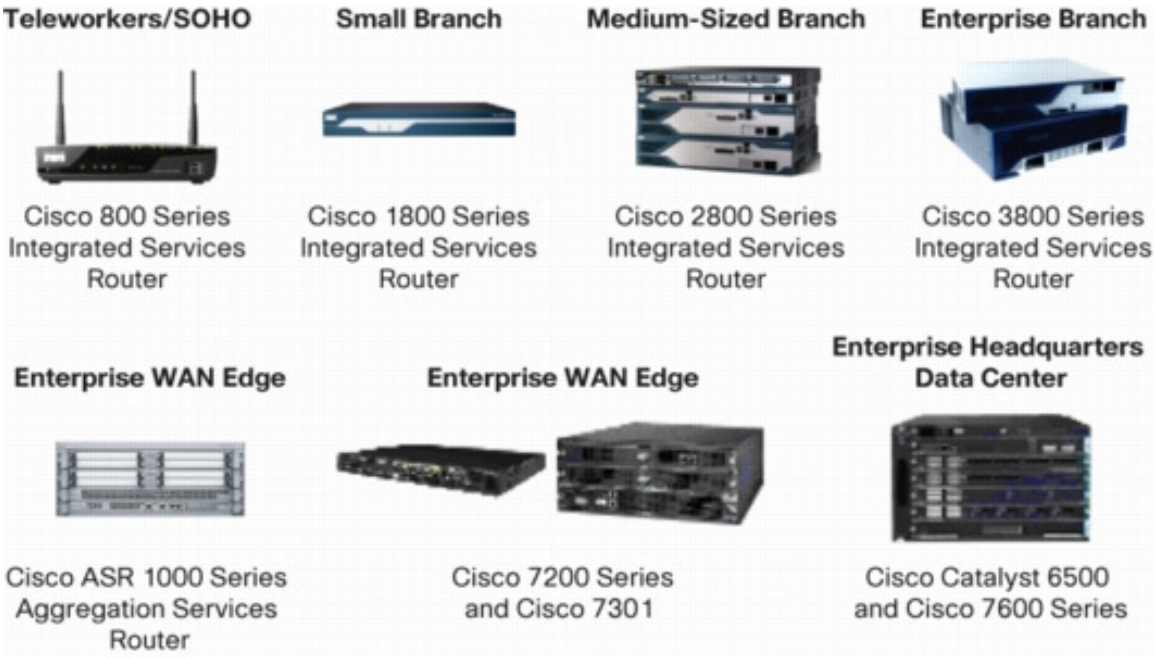


Figura 17 – Produtos Cisco capazes de fornecer um serviço VPN.

Estes produtos são capazes de fornecer um serviço de VPN com várias vantagens.

Uma vantagem é a capacidade de integração de VPNs IPSec e SSL, ou seja, num único equipamento são disponibilizadas VPNs de acesso remoto e/ou *site-to-site*.

Uma outra característica é a VPN *Dynamic Multipoint* (DMVPN), que permite o estabelecimento de VPNs IPSec *site-to-site*, de forma dinâmica. Isto é, descobre localizações remotas usando um protocolo de *routing standard*.

A VPN *Group Encrypted Transport* (GET VPN) é mais uma característica destes produtos e define-se como um novo tipo de VPN que elimina a necessidade dos túneis de uma VPN tradicional. O GET VPN proporciona uma ligação altamente escalável e de fácil gestão, sem a complexidade típica encontrada nos projectos de rede emalhada (*mesh* – ligação de todos *com* todos).

Uma outra vantagem é dispor de voz e de vídeo na VPN (V3PN). A V3PN integra telefonia IP, QoS e IPSec, fornecidos num serviço VPN *end-to-end*, que garante a entrega atempada do tráfego em aplicações sensíveis à latência, como a voz e o vídeo.

O serviço IPSec fiável e redundante é mais um benefício destes produtos, que proporciona uma rápida e escalável redundância para as sessões de VPN entre os sites remotos, com as soluções *stateless* e *stateful* disponíveis. As opções *Dead Peer Detection* (DPD), *Hot Standby Router Protocol* (HSRP), *Reverse Route Injection* (RRI) e comutação *Stateful* (SSO) ajudam a garantir o funcionamento de aplicações críticas.

Na tabela seguinte pode ver-se algumas características nos modelos mais comercializados.

Cisco VPN *Security Router*	**Máximo Túneis**	***Throughput* máxima**
Cisco 850 Series Integrated Services Router	5	8 Mbit/s
Cisco 870 Series Integrated Services Router	10	30 Mbit/s
Cisco 1841 Integrated Services Router with AIM-VPN/SSL-1	800	95 Mbit/s
Cisco 2801 Integrated Services Router with onboard VPN	150	50 Mbit/s
Cisco 2801 Integrated Services Router with AIM-VPN/SSL-2	1500	160 Mbit/s
Cisco 2811 Integrated Services Router with onboard VPN	200	55 Mbit/s
Cisco 3825 Integrated Services Router with onboard VPN	500	170 Mbit/s
Cisco 3845 Integrated Services Router with onboard VPN	700	180 Mbit/s
Cisco 3845 Integrated Services Router with AIM-VPN/SSL-3	2500	210 Mbit/s
Cisco 7301 Router with SA-VAM2+	5000	280 Mbit/s
Cisco 7200VXR Series Router and NPE-G1 with a single SA-VAM2+	5000	280 Mbit/s
Cisco Catalyst 6500 Series/Cisco 7600 Series VPN Bundle (includes one or more IPsec VPN SPAs)	16000	2,5-25 Gbit/s

Tabela 2 – Desempenho da VPN em Routers e Switches Cisco.

3.4. A Solução da Citrix

A Citrix apresenta uma solução dada pelo nome de Citrix *Access Gateway*.

Esta solução é uma aplicação de acesso seguro que fornece aos gestores de rede um controle minucioso ao nível aplicacional, e fornece acesso remoto aos utilizadores dessa mesma rede de qualquer lugar.

Este dispositivo permite o controlo de acesso e a limitação de funcionalidades a sessões, baseando-se na identidade do utilizador e no equipamento terminal. Estas características permitem uma maior segurança e protecção de dados. Para isso, utiliza a aplicação *SmartAccess*, disponibilizando uma grande flexibilidade para implementar políticas corporativas.

Esta *gateway* de acesso da Citrix é uma VPN SSL que permite todas as funcionalidades deste tipo de VPNs, tais como disponibilizar recursos para aceder aos ficheiros, ao *e-mail* e a outras necessidades do utilizador, independentemente da sua localização. Os *secure virtual desktops* e as aplicações são características adicionais desta *gateway*.

Com esta solução, a Citrix garante elevado desempenho e escalabilidade com mais de 10000 utilizadores simultaneamente no mesmo dispositivo.

Se a necessidade for um acesso mais rápido dos utilizadores para os *secure virtual desktops* e para as aplicações usam-se as soluções Citrix *Branch Repeater* em conjunto com a Citrix *Access Gateway*.

A Citrix *Access Gateway* está disponível no mercado em três versões: as edições *Standard*, *Advanced* e *Enterprise*.

A edição *Standard* é aconselhada a empresas com menos de 500 utilizadores remotos simultaneamente, e que não necessitem da implementação de políticas desenvolvidas.

A edição *Advanced* é aconselhada a empresas com menos de 500 utilizadores remotos simultaneamente, inclui a aplicação *SmartAccess* e o suporte a dispositivos móveis.

A edição *Enterprise* é a melhor solução de acesso seguro para ambientes de empresa, oferecendo escalabilidade e elevado desempenho, e incluindo as características de *SmartAccess* e de recuperação de falhas.

3.5. A Solução da Fortinet

As plataformas *FortiGate* incorporam as tecnologias de VPN Fortinet IPSec e SSL, assim como outras características de segurança, como por exemplo, as *firewalls*, os anti-vírus, os filtros de *Web*, e a prevenção de intrusões.

As soluções VPN *FortiGate* têm a capacidade de se adaptarem às necessidades do cliente, podem satisfazer todos os tipos de clientes.

A aplicação de gestão centralizada *FortiManager* oferece a capacidade de gerir implementações de VPN complexas, envolvendo milhares de sistemas *FortiGate* a partir de uma única consola.

Os processadores *FortiASIC* proporcionam um rápido desempenho desta solução, suportando tanto VPN SSL, como VPN IPSec.

Esta solução se for integrada com outras tecnologias de segurança Fortinet fornece uma protecção tanto ao nível da rede como ao nível dos conteúdos.

Com o uso das *FortiGate* existe um extenso suporte à autenticação do utilizador, e é possível utilizar vários protocolos de *tunneling* (IPSec, SSL, L2TP e PPTP).

Para preservar a largura de banda, estas plataformas podem criar prioridades no tráfego da VPN. As *FortiGate* são de fácil configuração.

3.6. A Solução da D-Link

A D-Link tem uma vasta gama de produtos para soluções de VPN e *firewall*.

Figura 18 – Equipamento DFL-210.

Apresenta-se uma solução da linha *NetDefend*, desenhada para responder a necessidades de VPN/*firewall,* mas que também tem a função de proteger os dados de ataques não desejados: DFL-210 *Network Security Firewall*.

O DFL-210 destina-se a soluções residenciais ou a pequenas empresas.

Este equipamento é uma solução de segurança integrada que junta funções de NAT, SPI *firewall*, características avançadas de filtragem, protecção IDS, gestão de largura de banda, e uma VPN.

O hardware do DFL-210 inclui quatro portas de LAN, uma porta de WAN e uma porta DMZ para suportar servidores locais. A porta DMZ também pode ser configurada como uma porta de WAN, no caso de a outra falhar.

Num ambiente empresarial pequeno, em termos de segurança, o DFL-210 tem várias características de *firewall* para gerir e manter uma rede segura e sem qualquer problema. Para fornecer capacidade de gestão de rede, este equipamento possui gestão remota, políticas de gestão de largura de banda, *Keyword Blocking*, políticas de acesso e SNMP. Para se poder monitorizar uma rede, este equipamento fornece alertas por *e-mail*, registos do sistema, verificações de consistência e estatísticas em tempo real.

O DFL-210 possui um Cliente e um Servidor de VPN integrados, suportando e gerindo até 100 diferentes configurações de VPNs. Esta solução suporta os protocolos de IPSec, PPTP e L2TP.

Nas opções mais avançadas de uma VPN, este equipamento suporta encriptação DES/3DES/AES/*Twofish*/*Blowfish*/CAST-128, gestão de chaves manual ou IKE/ISAKMP, modos de negociação *Quick/Main/Aggressive*, e autenticação VPN usando um servidor de RADIUS externo ou interno com uma base de dados de 500 utilizadores.

A configuração deste equipamento é bastante acessível, fornecendo uma intuitiva interface de utilizador.

A figura seguinte mostra uma grande e vasta variedade de soluções de VPN/*firewall*.

Figura 19 – Vários modelos da D-Link para soluções de VPN.

Capítulo 4

Desenho da Solução Proposta

Após o estudo das tecnologias e protocolos existentes nas *Virtual Private Networks* verificou-se que não existe numa tecnologia específica para prover redundância nesta área. Por esse motivo surge a escolha de duas tecnologias que, apesar de diferentes, são as mais utilizadas actualmente, pelas suas potencialidades e abrangentes áreas de aplicação, são elas as VPNs SSL e IPSec. Contudo estas têm as suas vantagens e desvantagens em áreas importantes como a segurança, o desempenho, a complexidade e o custo.

A grande diferença entre as VPNs SSL e IPSec está na segurança que disponibilizam. Em alguns casos a segurança é o principal critério para se adoptar uma tecnologia em concreto. A VPN SSL tem uma segurança moderada devido a ser possível estabelecer o túnel a partir de qualquer computador. Na VPN IPSec a segurança é um ponto forte devido ao túnel ser criado após a validação de vários critérios, como por exemplo, o endereço IP, as fases de autenticação e a aplicação estar associada à encriptação.

A aplicação do SSL assenta em serviços disponibilizados via navegador *Web*, *e-mail* e partilha de ficheiros. No caso de uma VPN IPSec, a sua aplicação é baseada em serviços IP, tais como, FTP, partilha de impressoras, acesso a bases de dados.

Ambos os protocolos suportam autenticação. Deste modo é garantida a autenticidade de cada extremidade (cliente e servidor) para que ocorra o estabelecimento do túnel VPN. Ao contrário da encriptação, tanto o IPSec quanto o SSL podem utilizar as mesmas técnicas de autenticação. Ambos os protocolos podem utilizar os seguintes mecanismos de autenticação: *login* e senha, *login* e *token* ou certificados digitais.

Uma das vantagens do IPSec é que este opera na camada de rede, garantindo a segurança da informação entre as duas pontas do túnel VPN. Os utilizadores remotos têm acesso aos recursos locais do extremo do túnel como se eles estivessem fisicamente nesse local.

O SSL usa o navegador *Web* (*Internet Explorer*, *Netscape* ou *Firefox*) como interface para os utilizadores remotos, o que o torna vantajoso, na medida em que a maioria dos utilizadores está familiarizado com o seu uso e encontra-se disponível em quase todos os sistemas operativos, como o Windows, o Linux e o MAC OS.

Uma desvantagem do SSL é que este opera na camada de aplicação, limitando o acesso a recursos da rede local, como por exemplo a partilha de impressoras, o acesso a bases de dados e a aplicações especificas.

A nível de custos, a solução SSL torna-se a menos dispendiosa, porque apenas é necessário o equipamento específico no destino, pois na origem, basta apenas uma ligação à Internet. No caso do IPSec, aplicando cenários de redundância maiores, os custos associados serão enormes, quer em equipamentos, quer em circuitos de interligação.

Foi equacionada a redundância através do DNS, ou seja, na criação do túnel em vez da colocação de um IP de destino colocar-se-ia um nome, ao qual estavam associados dois endereços IP.

Contudo esta solução não é viável devido ao facto de apenas ser possível a adição de entradas em DNS na Internet através da compra de domínios públicos. Uma outra forma era a adição de entradas estáticas (ficheiro *hosts*) na própria máquina que acede ao túnel. Desta forma não teríamos redundância de uma forma simples e sem necessidade de configurações específicas, sendo esta a principal vantagem da VPN SSL.

4.1. Cenário Um – VPN SSL *Clientless*

A primeira abordagem ao problema irá ser feita de uma forma simplista, ou seja, antes da implementação de redundância do serviço VPN, este serviço irá ser testado por si só.

No primeiro cenário irá ser implementada uma VPN SSL *clientless*, também designada de *webvpn*, fazendo parte das implementações mais recentes e simples.

O utilizador remoto irá aceder a uma página da Internet e aí será pedida uma autenticação (*username/password*). Depois de autenticado, o utilizador ficará ligado através de um túnel seguro SSL ao destino. A partir daí terá acesso aos recursos pré-configurados pelo gestor de rede, como por exemplo, o *e-mail* – *Web-access*, o servidor *Web*, a partilha de ficheiros.

Se houver uma quebra na ligação da VPN, como por exemplo, avaria do router, quebra na ligação à Internet na origem ou no destino, ou até mesmo uma falha no servidor Web, o serviço fica inoperacional. Uma das desvantagens desta solução é não existir qualquer tipo de redundância aplicada.

Uma das vantagens da criação de um túnel SSL é estabelecer-se uma comunicação segura cliente-servidor sobre a camada de transporte TCP.

A figura seguinte mostra o esquema da solução proposta.

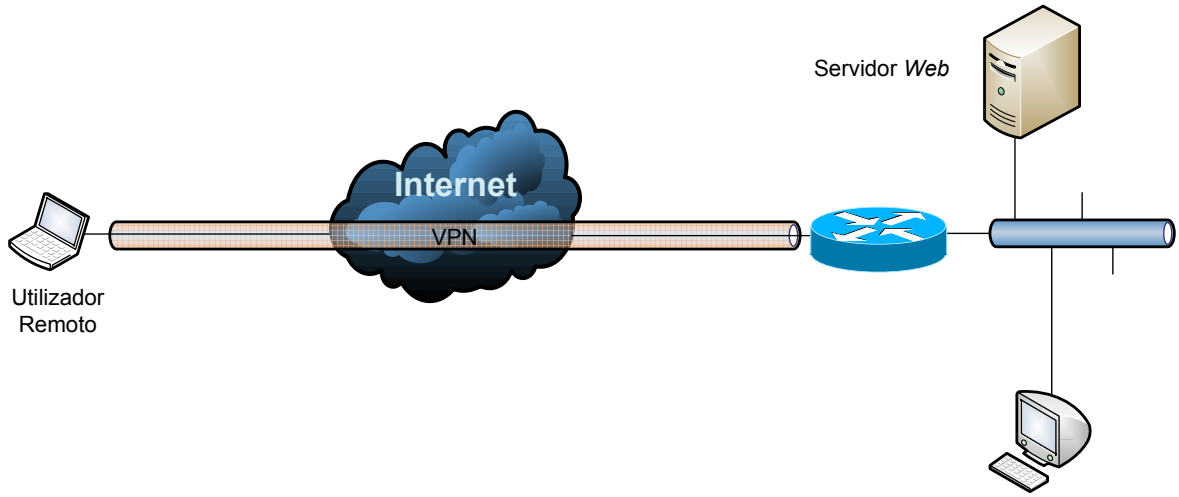


Figura 20 – Esquema de rede do primeiro cenário – VPN SSL – *host-to-net.*

Para esta solução será utilizado um router Cisco 877, ligado à Internet através de uma linha ADSL, um PC de testes e um servidor *Web*. O IP da ligação à Internet terá de ser fixo, pois o utilizador remoto irá ligar-se sempre pelo mesmo IP.

4.2. Cenário Dois – VPN IPSec Redundante (circuito)

O cenário seguinte apresenta uma solução já redundante, contudo o tipo de VPN é diferente do cenário anterior, pois passa-se de uma solução *host-to-net*, onde um utilizador liga-se a uma rede remota, para uma solução *net-to-net*, onde o utilizador encontra-se numa rede local e irá ligar-se a uma rede remota sem a necessidade de requisitos. Ou seja, não será o utilizador responsável pela ligação VPN, mas sim as *gateways* de cada uma das redes, local e remota.

Neste cenário os dois circuitos entre os equipamentos remoto e local vão assegurar a redundância da VPN. Desde modo, caso um dos circuitos falhe o utilizador irá conseguir comunicar com o destino e aceder aos recursos da rede remota.

Uma das limitações desta arquitectura é a inoperacionalidade do serviço caso haja uma falha de qualquer um dos routers. A vantagem deste cenário é ser uma solução transparente ao utilizador. Quer isto dizer, que se houver uma quebra na ligação ISP1, o serviço será reposto pela ligação ISP2, sem que o utilizador proceda a qualquer acção, ou vice-versa.

Esta passagem do ISP1 para o ISP2 deve-se ao uso do protocolo OSPF, que permite a divulgação de rotas nos circuitos em funcionamento. O ISP1 é definido com o circuito principal e o ISP2 é o circuito redundante pelas configurações do próprio protocolo.

O protocolo IPSec opera na camada de rede, garantindo a segurança da informação entre a origem e o destino, e é independente do tipo de tráfego que transporta.

O esquema proposto é o seguinte:

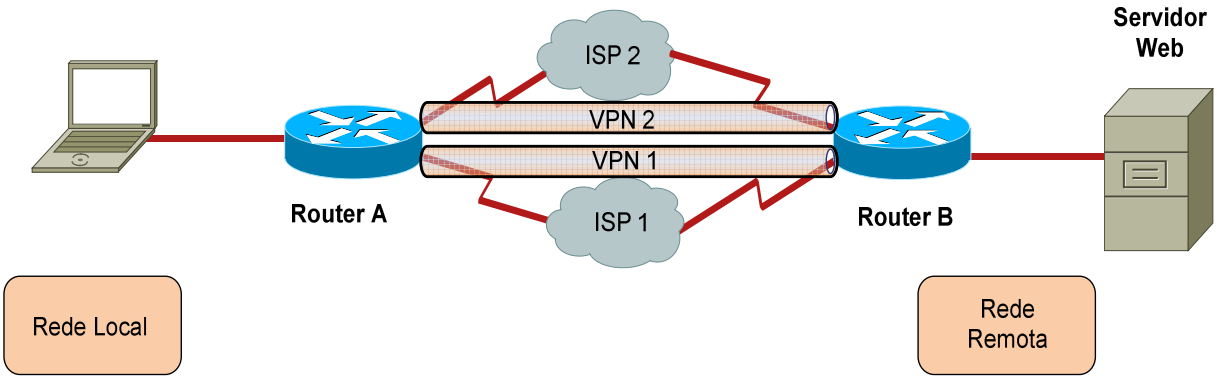


Figura 21 – Esquema de rede do segundo cenário – VPN IPSec Redundante – *net-to-net.*

Para esta solução serão utilizados dois routers Cisco 1841, um PC de testes e um servidor *Web.*

4.3. Cenário Três – VPN IPSec Redundante (equipamento e circuito)

No caso do cenário três irá ser implementada uma solução onde existe tanto a redundância de circuitos como a redundância de equipamentos. No cenário dois apenas será implementada a redundância de circuitos entre os dois locais.

Este cenário irá ter um maior grau de fiabilidade do serviço, visto que será assegurado, por dois circuitos entre dois equipamentos na rede remota. Desde modo, caso um dos circuitos falhe ou um dos routers remotos fique inoperacional, o utilizador irá conseguir comunicar com o destino e aceder aos recursos da rede remota.

De modo a garantir a redundância também do lado da rede local remota, utilizou-se o protocolo VRRP, que permite que existam dois equipamentos com o mesmo IP (virtual) na rede local. Sendo assim a *gateway* aplicada a todas as máquinas dessa rede deverá ser o IP virtual configurado nos dois routers que fornecem ligações aos ISP1 e ao ISP2.

O esquema proposto é o seguinte:

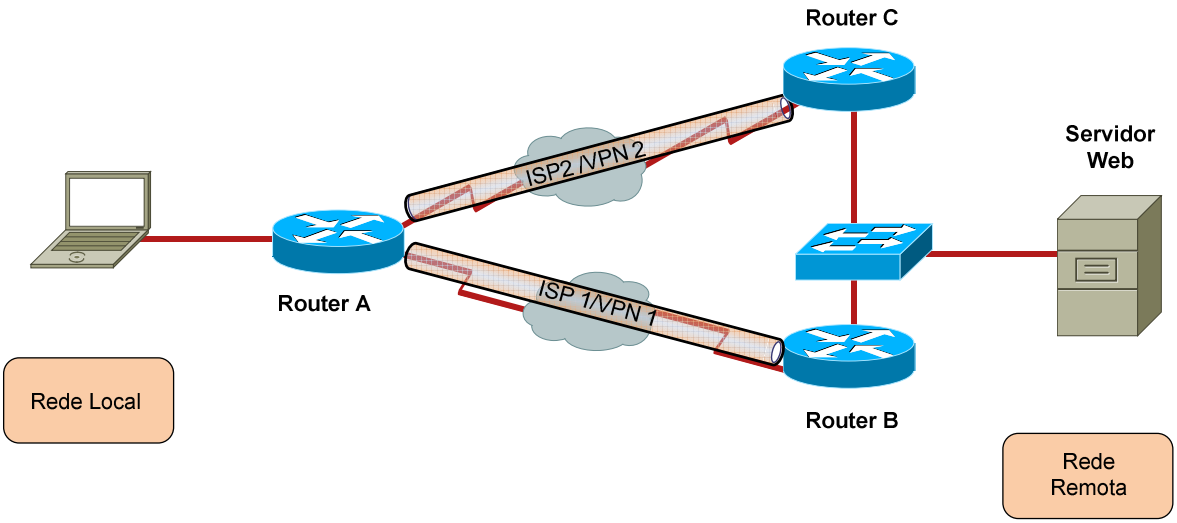


Figura 22 – Esquema de rede do terceiro cenário – VPN IPSec Redundante (equipamento e circuito) – *net-to-net.*

Para esta solução serão utilizados três routers Cisco 1841, um PC de testes e um servidor *Web.*

Capítulo 5

Implementação

Para a implementação do primeiro cenário, configurou-se o router Cisco 877 conforme as configurações do Anexo A. Este anexo contém apenas as configurações necessárias para um acesso à Internet.

O passo seguinte foi a criação do túnel SSL, através de uma aplicação da Cisco designada por SDM (*Security Device Manager*). Todos passos necessários estão expostos no Anexo B. No final de todas as configurações, o router gera a configuração apresentada no Anexo C.

Para esta implementação foi seguido o esquema seguinte.

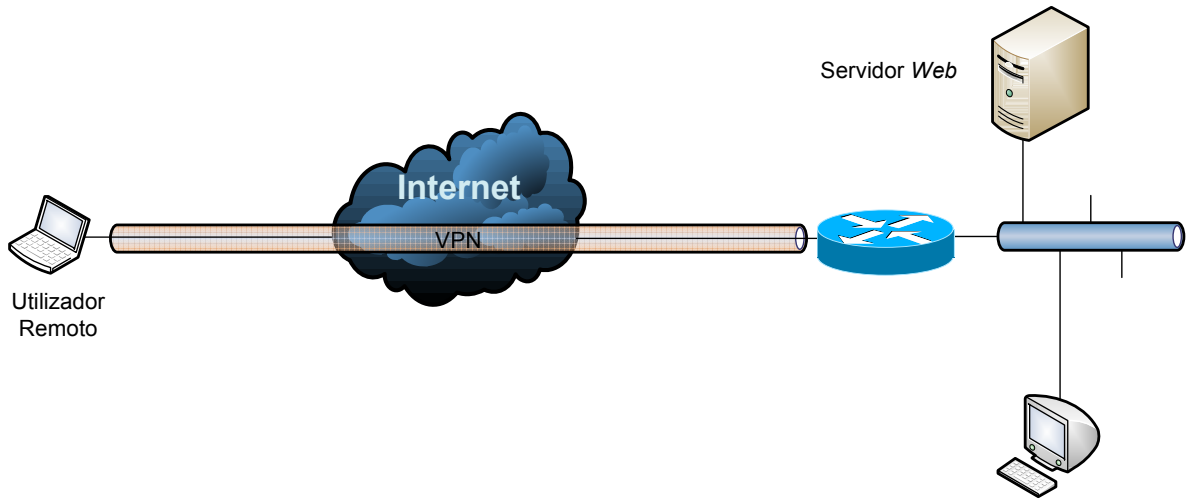
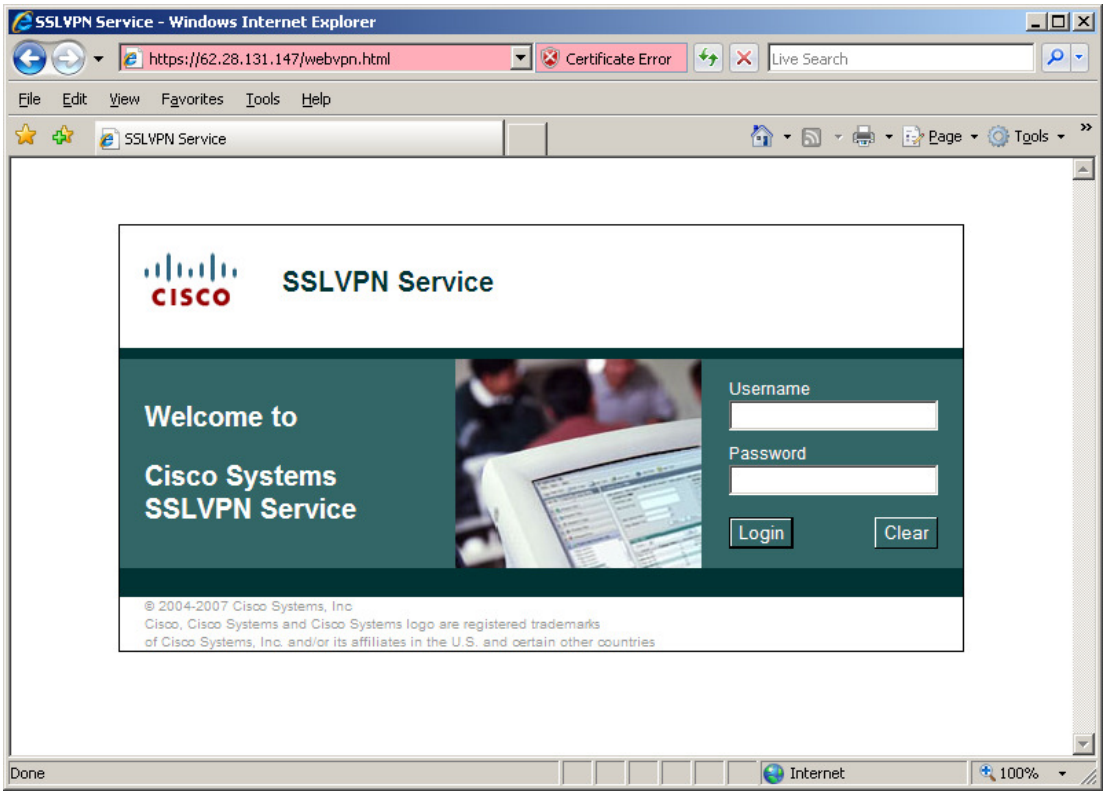
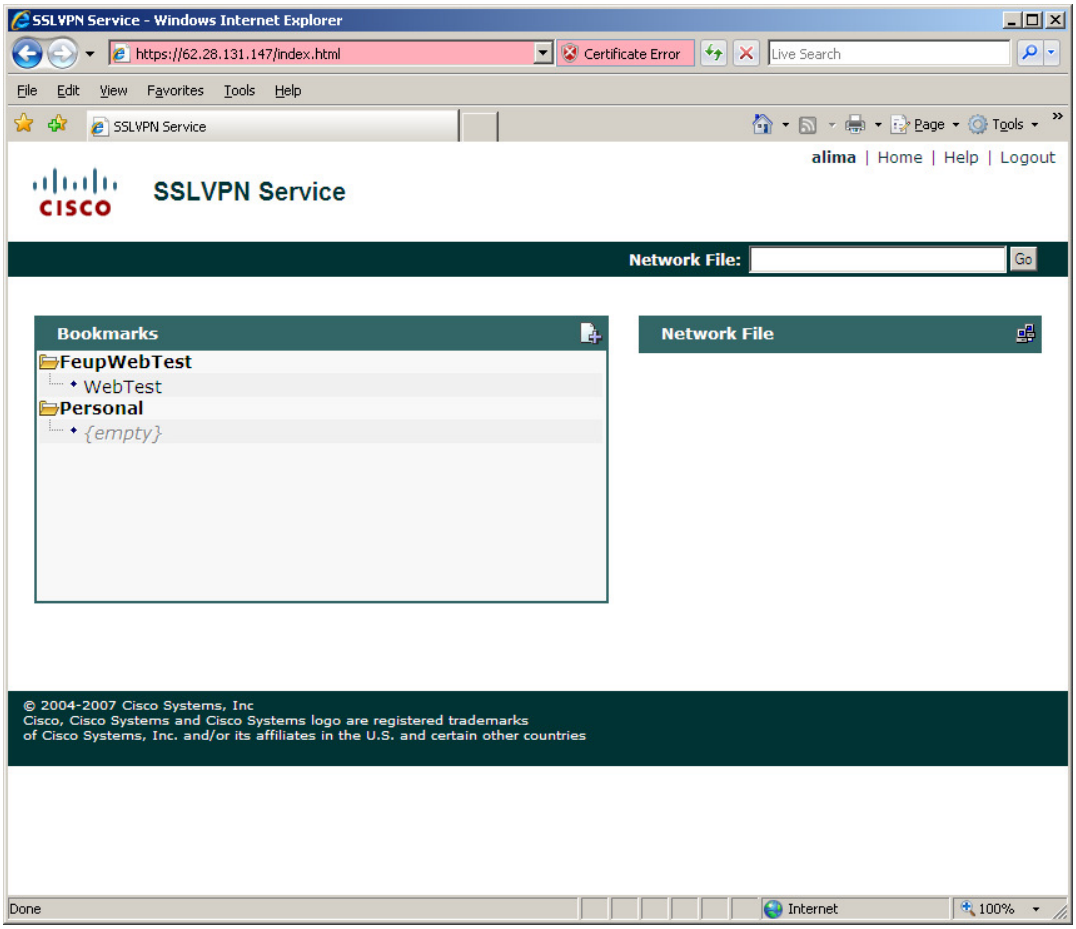


Figura 23 – Esquema de rede implementado no primeiro cenário.

Para se poder verificar os resultados e testar a ligação, acede-se à página pelo navegador *Web*: https://62.28.131.147



Efectuando a autenticação via *username* e *password*, aparece como página de entrada já no túnel SSL VPN o ecrã seguinte.



No apontador *WebTest* aparece a página *Web* da dissertação que está alojada no servidor que foi definido com o IP 192.168.1.3.

Desta forma foi estabelecida com sucesso a ligação http ao IP 192.168.1.3, utilizando um túnel SSL VPN.

Depois de estabelecido o cenário um partiu-se para a implementação do cenário dois, em que a redundância é implementada.

O diagrama de rede seguinte mostra uma solução de um serviço VPN redundante, que foi estudado e testado.

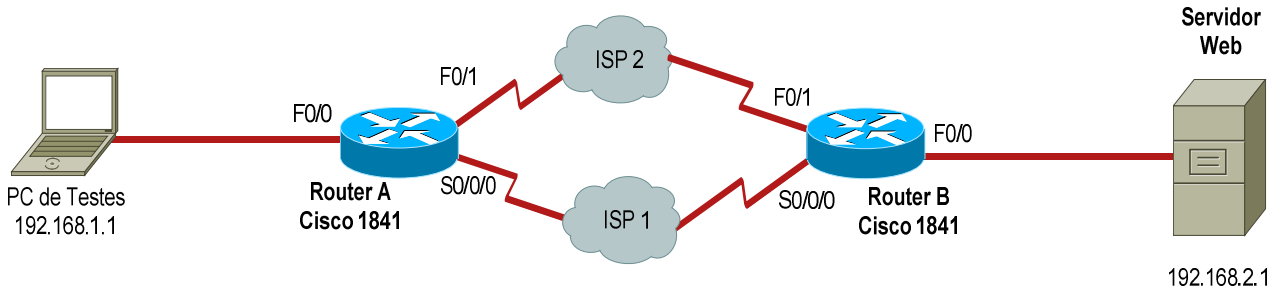


Figura 24 – Diagrama de rede testado no cenário dois.

Este cenário deverá garantir o acesso ao servidor *Web*, em caso de falha do ISP1 ou do ISP2, através de túneis seguros IPSec estabelecidos entre os dois routers.

Cada túnel irá utilizar um ISP distinto.

Como não foi possível, em ambiente de laboratório, disponibilizar 4 ligações WAN (2 para cada router) a ISPs distintos ou mesmo a um só, os testes foram realizados utilizando os dois routers ligados "costas com costas" através de interfaces *Serial* e *FastEthernet*.

O ISP1 foi simulado através da ligação de cabos com interface V.35, macho e fêmea, emulando uma ligação Frame *relay*.

O ISP2 é fornecido através de uma ligação com um cabo UTP cruzado, entre as interfaces *FastEthernet*0/1 dos equipamentos, simulando uma ligação Ethernet.

A foto mostra o cenário real de testes.

Figura 25 – Laboratório de testes.

O diagrama seguinte mostra o ambiente real de testes.

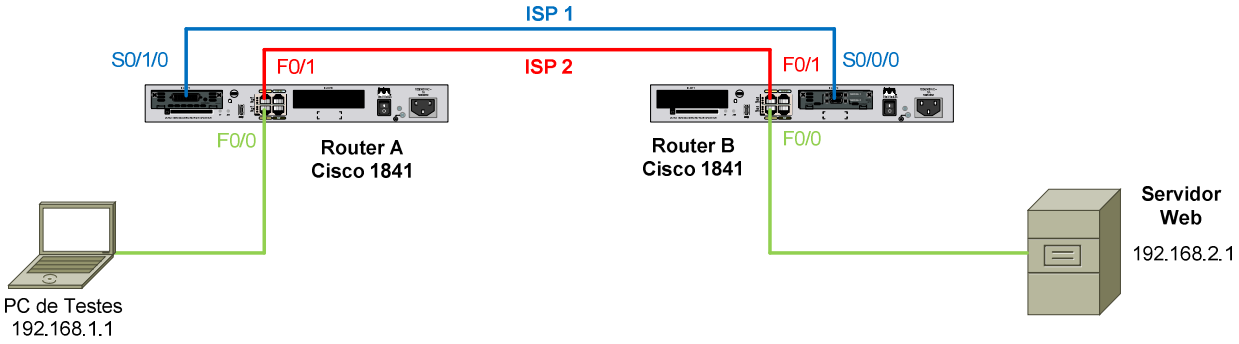


Figura 26 – Diagrama real de testes do cenário dois.

Os IPs atribuídos foram os seguintes:

Router A
FastEthernet 0/0 – 192.168.1.254/24
Serial 0/1/0 – 10.1.1.1/30
FastEthernet 0/1 – 10.2.2.1/30
Túnel 1 – 10.10.10.1/30
Túnel 2 – 10.20.20.1/30

Router B
FastEthernet 0/0 – 192.168.2.254/24
Serial 0/0/0 – 10.1.1.2/30
FastEthernet 0/1 – 10.2.2.2/30
Túnel 1 – 10.10.10.2/30
Túnel 2 – 10.20.20.2/30

As configurações utilizadas nos dois routers estão no Anexo D.

Mostrando que as duas ligações, ISP1 e ISP2 estão operacionais, os comandos seguintes verificam que os dois túneis estão estabelecidos e a comunicar através do protocolo de *routing* OSPF.

```
Router_A#sh ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.2540    FULL/  -        00:00:39    172.16.255.102  Tunnel2
192.168.2.2540    FULL/  -        00:00:39    172.16.255.2    Tunnel1
```

O caminho utilizado (ISP1) apresenta os seguintes *hops*:

```
Router_A#traceroute 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 10.10.10.2 4 msec 4 msec 4 msec
  2 192.168.2.1 4 msec 4 msec 4 msec
```

Como se pode verificar o primeiro *hop* é o Túnel 1.

Os testes seguintes mostram a redundância: o ISP1 fica inoperacional e passa-se para o ISP2.

```
*Dec 30 21:36:45.679: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to
down
*Dec 30 21:36:46.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1/0, changed state to down
*Dec 30 21:37:19.067: %OSPF-5-ADJCHG: Process 1, Nbr 172.22.22.22 on Tunnel1
from FULL to DOWN, Neighbor Down: Dead timer expired
Router_A#
Router_A#
Router_A#sh ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.22.22.22      0   FULL/  -        00:00:39    172.16.255.102  Tunnel2
```

Apenas o túnel 2 está operacional.

O caminho utilizado (ISP2) apresenta os seguintes *hops*:

```
Router_A#trace 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 10.20.20.2 4 msec 4 msec 4 msec
  2 192.168.2.1 4 msec 4 msec 4 msec
```

Como se pode verificar o primeiro *hop* é o Túnel 2.

De seguida, o ISP1 vai voltar a ficar operacional.

```
*Dec 30 21:38:35.351: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to
up
*Dec 30 21:38:36.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1/0, changed state to up
*Dec 30 21:38:39.083: %OSPF-5-ADJCHG: Process 1, Nbr 172.22.22.22 on Tunnel1
from LOADING to FULL, Loading Done
Router_A#sh ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.22.22.22      0   FULL/  -        00:00:37    172.16.255.102  Tunnel2
172.22.22.22      0   FULL/  -        00:00:34    172.16.255.2    Tunnel1
```

O túnel 1 fica novamente operacional.

O caminho seleccionado passa novamente a utilizar o ISP1.

```
Router_A#traceroute 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 10.10.10.2 4 msec 4 msec 4 msec
  2 192.168.2.1 4 msec 4 msec 4 msec
```

O primeiro *hop* é o Túnel 1.

Fazendo testes a partir do PC de testes e utilizando a aplicação PingPlotter, revela-se que a redundância do ISP1 para o ISP2 leva a uma quebra de serviço de sensivelmente 17 segundos.

Figura 27 – Gráfico temporal relativo à conectividade através do túnel 1.

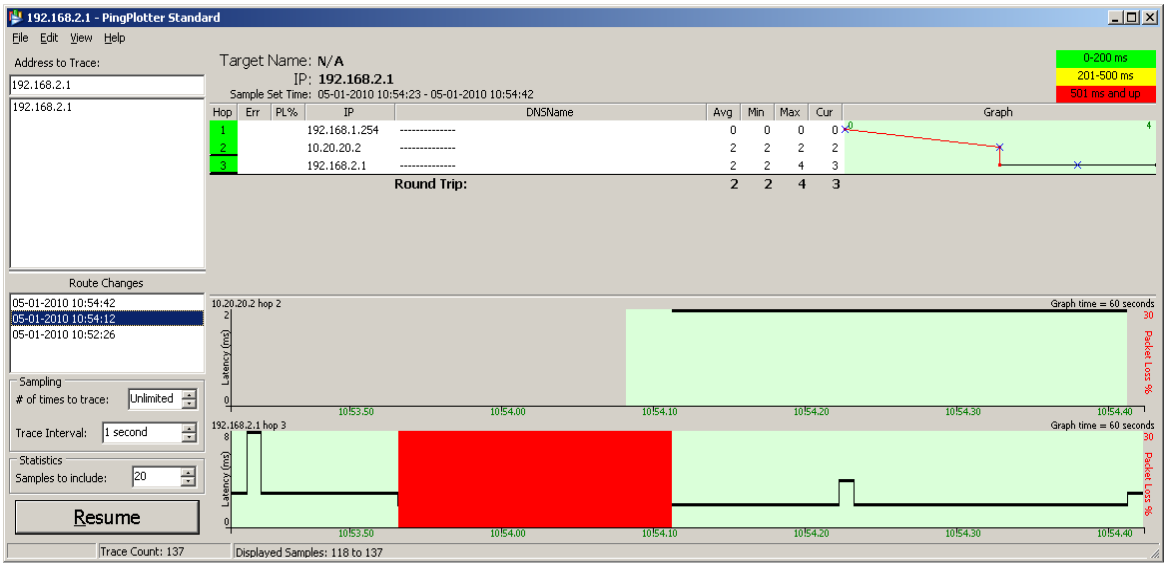


Figura 28 – Gráfico temporal relativo à conectividade através do túnel 2.

Parte-se agora para o terceiro cenário, onde é implementada uma solução onde existe tanto a redundância de circuitos como a redundância de equipamentos. O cenário anterior mostra uma solução redundante onde apenas os circuitos são redundantes, ou seja, caso o router do lado do servidor *Web* fique inoperacional o serviço é quebrado.

No terceiro cenário é adicionado um terceiro router. Deste modo a solução passa a ser redundante quer no circuito, quer nos equipamentos do site crítico.

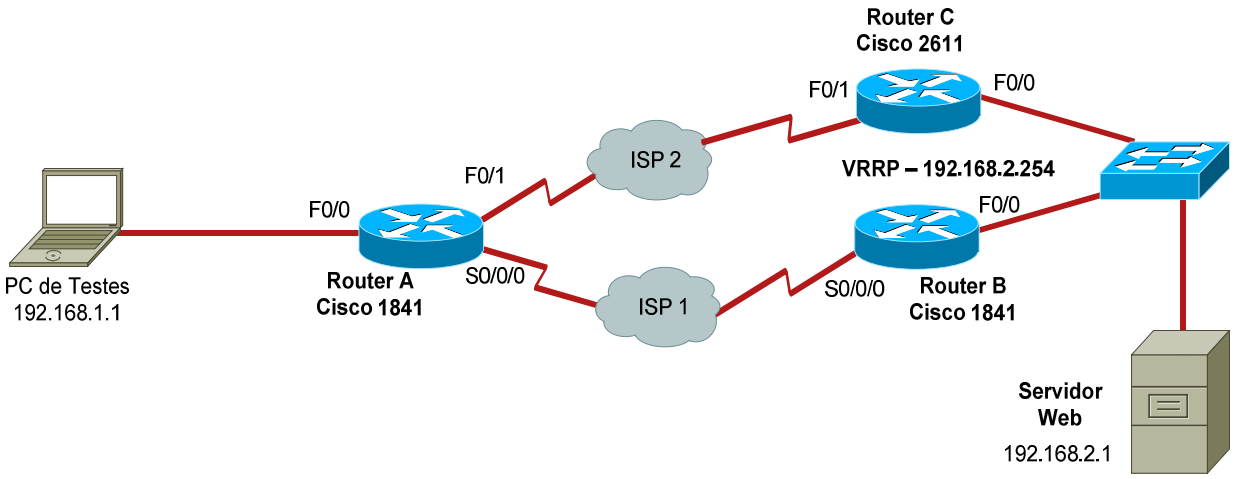


Figura 29 – Diagrama de rede testado no cenário três.

Este cenário deverá garantir o acesso ao servidor *Web*, em caso de falha do ISP1/*Router* B ou do ISP2/*Router* C, através de túneis seguros IPSec, estabelecidos entre o *Router* A e os dois routers B e C. Cada túnel irá utilizar um ISP e router distinto.

Tal como no cenário anterior, devido a não ser possível, disponibilizar 4 ligações WAN a ISPs distintos ou mesmo a um só, o ambiente de testes em laboratório foi realizado utilizando os routers ligados "costas com costas" através de interfaces *Serial* e *FastEthernet*.

A ligação através do ISP1 (*Router* A – *Router* B) foi simulada através da ligação de cabos com a interface V.35, macho e fêmea, emulando uma ligação *Frame relay*.

O *Router* A e *Router* C (ligação do ISP2) ficam conectados através de uma ligação com um cabo UTP cruzado, entre as *FastEthernet* 0/1 dos equipamentos, simulando uma ligação *Ethernet*.

O diagrama seguinte mostra o ambiente real de testes.

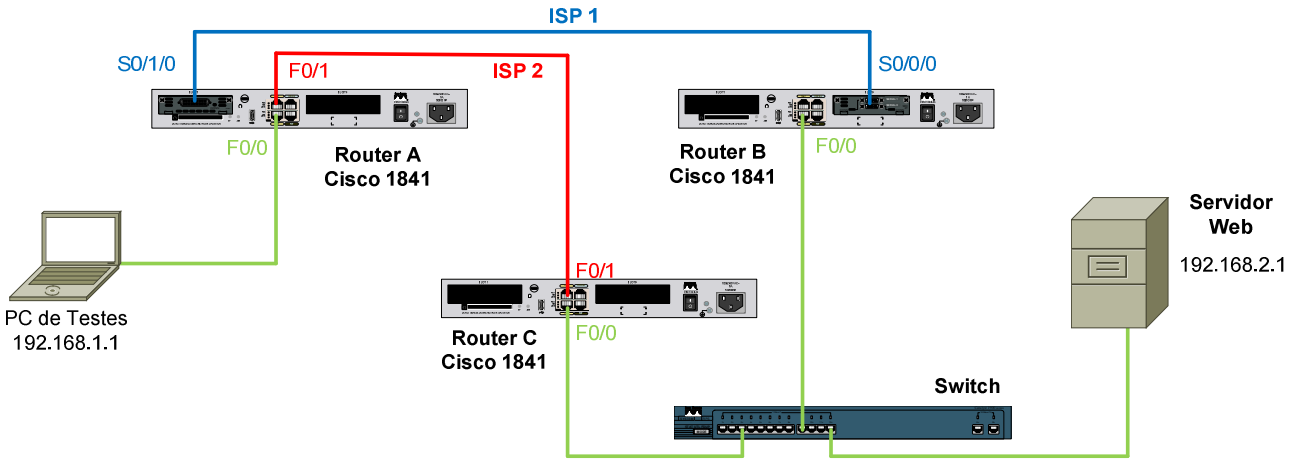


Figura 30 – Diagrama real de testes do cenário três.

Os IPs atribuídos foram os seguintes:

Router A
FastEthernet 0/0 – 192.168.1.254/24
Serial 0/1/0 – 10.1.1.1/30
FastEthernet 0/1 – 10.2.2.1/30
Túnel 1 – 10.10.10.1/30
Túnel 2 – 10.20.20.1/30

Router B
FastEthernet 0/0 – 192.168.2.253/24
Serial 0/0/0 – 10.1.1.2/30
Túnel 1 – 10.10.10.2/30

Router C
FastEthernet 0/0 – 192.168.2.252/24
FastEthernet 0/1 – 10.2.2.2/30
Túnel 2 – 10.20.20.2/30

Os Routers B e C encontram-se ligados no mesmo local, ou seja, na mesma rede local. Deste modo terá de existir um protocolo que tornará os dois routers redundantes entre si, permitindo que possam ter o mesmo IP (virtual), que será o *gateway* da rede local. Para isso, usa-se o protocolo VRRP (*Virtual Router Redundancy Protocol*). Assim, o router onde estiver configurada a prioridade mais elevada será o *Master*, ficando com a função de encaminhar o tráfego entre LAN e WAN. O *Slave* permanecerá em *backup* até que o *Master* deixe de estar operacional. Quando o *Master* fica inoperacional, o router *Slave* assume a função de *Master*.

As configurações utilizadas no *Router* A são exactamente as mesmas que as utilizadas no cenário anterior.

Relativamente às configurações do *Router* B do cenário anterior, passam a não existir configurações relativas ao ISP2 (interface, encriptação, túneis). No Anexo E encontram-se as configurações dos routers B e C do terceiro cenário.

Mostrando que as duas ligações, ISP1 e ISP2 estão operacionais, os comandos seguintes verificam que os dois túneis estão estabelecidos e a comunicar através do protocolo de *routing* OSPF.

```
Router_A#sh ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.252     0   FULL/  -        00:00:39    10.20.20.2      Tunnel2
192.168.2.253     0   FULL/  -        00:00:37    10.10.10.2      Tunnel1
```

O caminho utilizado (ISP1) apresenta os seguintes *hops*:

```
Router_A#traceroute 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 10.10.10.2 4 msec 4 msec 4 msec
  2 192.168.2.1 4 msec 4 msec 4 msec
```

Como se pode verificar o primeiro *hop* é o Túnel 1.

Os testes seguintes mostram a redundância: o ISP1 ou o *Router* B ficam inoperacionais e passa-se para o ISP2 e para o *Router* C.

```
*Jan 13 13:59:20.435: %LINK-5-CHANGED: Interface Serial0/1/0, changed state to
administratively down
*Jan 13 13:59:21.435: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1/0, changed state to down
*Jan 13 13:59:34.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1,
changed state to down
*Jan 13 13:59:34.619: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.253 on Tunnel1
from FULL to DOWN, Neighbor Down: Interface down or detached
Router_A#
Router_A#
Router_A#sh ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.252     0   FULL/  -        00:00:38    10.20.20.2      Tunnel2
```

Apenas o túnel 2 está operacional.

O caminho utilizado (ISP2) apresenta os seguintes *hops*:

```
Router_A#traceroute 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 10.20.20.2 0 msec 0 msec 4 msec
  2 192.168.2.1 4 msec 4 msec 0 msec
```

Como se pode verificar o primeiro *hop* é o Túnel 2.

De seguida, o ISP1 vai voltar a ficar operacional.

```
*Jan 13 14:10:20.795: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to
up
*Jan 13 14:10:21.795: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1/0, changed state to up
*Jan 13 14:10:24.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1,
changed state to up
*Jan 13 14:10:24.639: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.253 on Tunnel1
from LOADING to FULL, Loading Done
Router_A#
Router_A#sh ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.252     0   FULL/  -        00:00:37    10.20.20.2      Tunnel2
192.168.2.253     0   FULL/  -        00:00:37    10.10.10.2      Tunnel1
```

O túnel 1 fica novamente operacional.

O caminho seleccionado passa novamente a utilizar o ISP1.

```
Router_A#traceroute 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 10.10.10.2 4 msec 4 msec 4 msec
  2 192.168.2.1 4 msec 4 msec 4 msec
```

O primeiro *hop* é o Túnel 1.

Fazendo testes através do PC de testes e utilizando a aplicação PingPlotter, revela-se que a redundância do ISP1 para o ISP2 leva a uma quebra de serviço de sensivelmente 17 segundos.

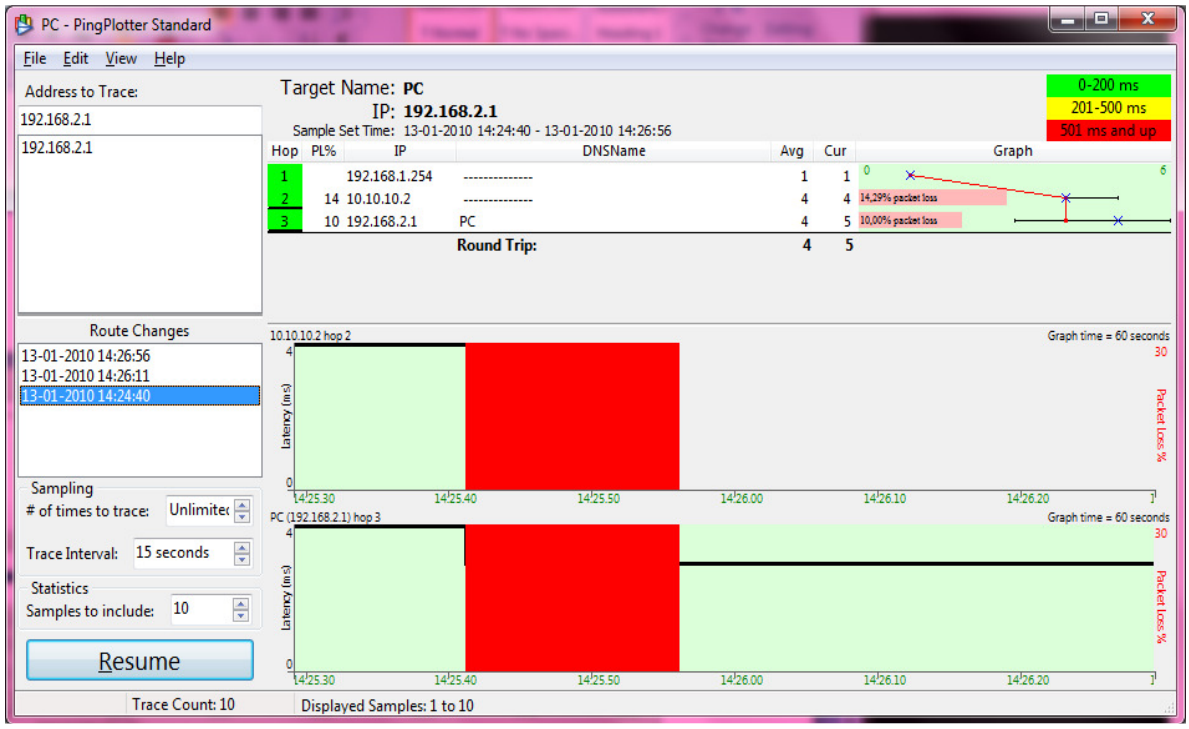


Figura 31 – Gráfico temporal relativo à conectividade através do túnel 1.

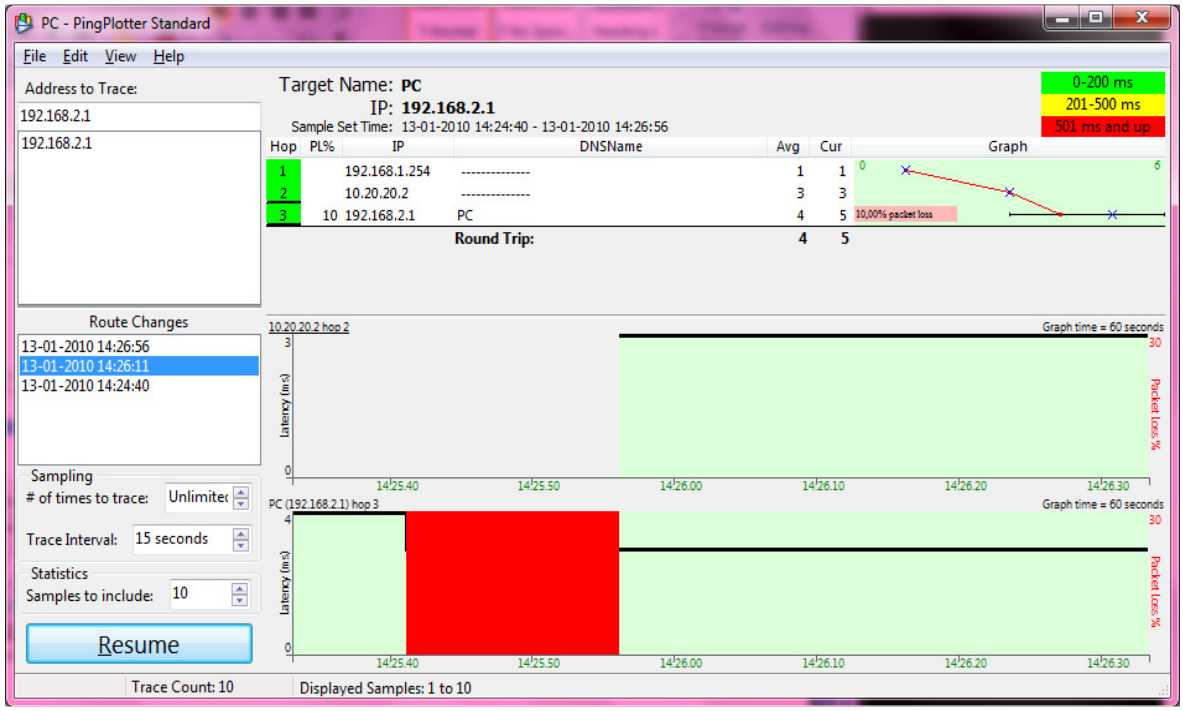
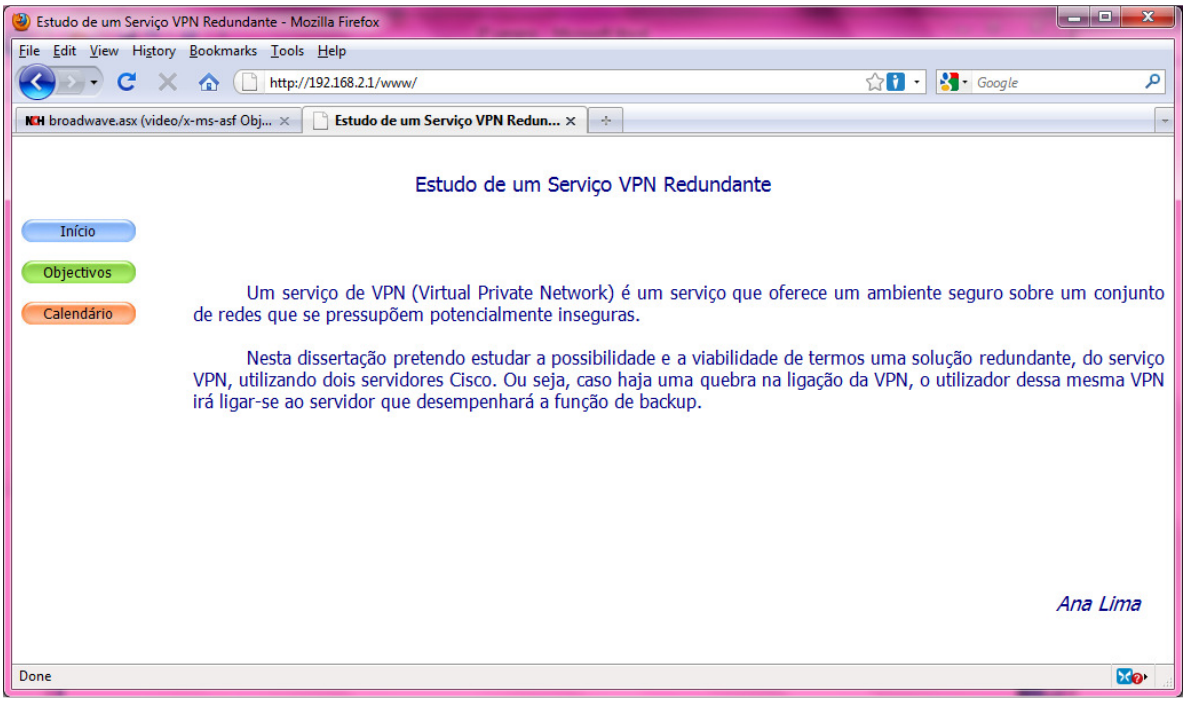
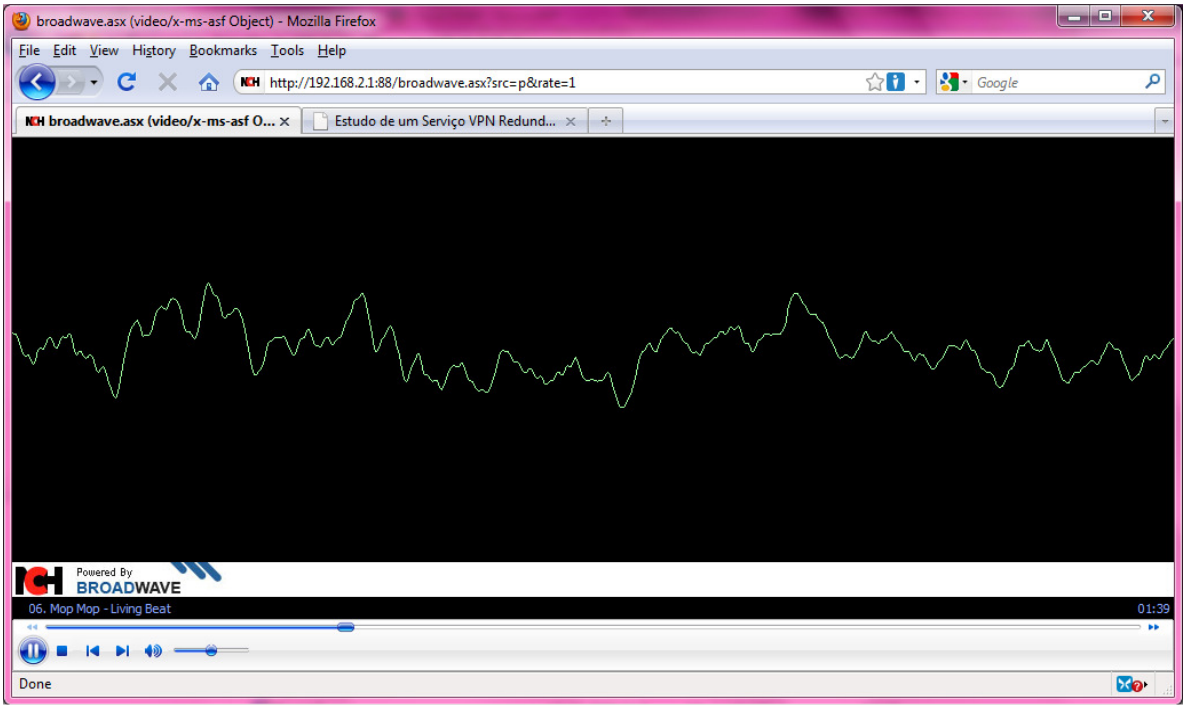


Figura 32 – Gráfico temporal relativo à conectividade através do túnel 2.

A nível aplicacional, e sendo a máquina de destino um servidor *web*, este servidor disponibilizou a página referente a esta dissertação.



Como esta página é estática, colocou-se no servidor *Web* uma aplicação de *streams* de áudio *on-line*, que também está disponível via *Web*. A aplicação de *streams* de áudio serve para demonstrar a continuidade do serviço da VPN.



Como existe um *buffer* que vai armazenando a *stream* de áudio, quando a redundância é activada não ocorre nenhuma perda a nível do áudio na transmissão. Mesmo existindo uma queda de 17 segundos na conectividade entre os dois sites remotos, este intervalo de tempo não é suficiente para se verificar a falha no serviço.

Deste modo, este cenário redundante é uma boa solução para um serviço de *streams* de áudio ou vídeo, como por exemplo uma rádio *on-line*.

Capítulo 6

Conclusões

O estudo da tecnologia VPN tornou-se bastante interessante, mas um pouco vasto devido ao leque de tipos de VPNs, criptografias, modos de acesso e equipamentos existentes. A VPN SSL e IPSec salientam-se de todas as outras. A VPN SSL é simples e eficaz. A VPN IPSec é um *standard* na tecnologia garantindo acesso a inúmeros recursos de rede.

A nível da redundância em VPNs as soluções estão mais desenvolvidas para cenários de WAN ou *net-to-net*, como é o caso dos *backbones* de grandes operadores de telecomunicações. Neste campo é imprescindível a fiabilidade e a segurança, devido à necessidade da separação do tráfego dos inúmeros clientes dentro do mesmo meio físico, bem como a garantia de um serviço sempre disponível, daí a importância da redundância.

Para grandes empresas a questão da redundância nas VPNs torna-se mais importante para os casos de acesso remoto, pois na WAN é o operador que terá de garantir redundância. Para estes cenários podem-se encontrar, como uma solução bastante viável, os agregadores e as *firewalls* da Cisco, como por exemplo, o ASA 5500, em que podem criar vários tipos de redundância conforme as necessidades.

Uma boa solução para as PMEs, mesmo em termos económicos, são os produtos da D-Link, como é o caso do DFL-210. Estes, apesar de não possuírem redundância por si só, preenchem as necessidades de acesso VPN remoto a este tipo de empresas.

Nas VPNs *host-to-net* os problemas encontrados relacionam-se com o tipo de ligação que é estabelecida. Na implementação do primeiro cenário, o utilizador remoto liga-se à VPN SSL, via *Web,* a um endereço IP público único.

No segundo e terceiro cenários, o estudo aprofundou-se numa solução de VPN *net-to-net* redundante. Partindo do pressuposto que teriam de ser usados dois caminhos distintos e redundantes entre si, foram criados túneis IPSec para o efeito e aplicado o protocolo de *routing* OSPF para que os encaminhamentos IP deixassem de existir na quebra de conectividade de cada túnel. Os resultados foram satisfatórios, pois a quebra da conectividade de um túnel apenas provoca 17 segundos de indisponibilidade até à activação da redundância. Em aplicações, como o *streaming* de áudio verificou-se que devido ao *buffer* existente a quebra não é perceptível para o utilizador, o que torna esta solução bastante apropriada para o efeito.

Como foi demonstrado em toda esta dissertação é possível e viável existir um serviço VPN que assente numa arquitectura redundante. Quer isto dizer, que caso haja uma quebra na ligação da VPN, o utilizador continuará a ter acesso aos serviços disponibilizados pela VPN. A sensibilidade do utilizador a esta quebra de ligação dependerá do tipo de serviço que esteja a ser utilizado.

Trabalho Futuro

No trabalho que desempenho no dia-a-dia, inúmeras questões são levantadas sobre a redundância existente nas redes de telecomunicações.

Tendo como lema que não existem clientes menos importantes, e que todos os serviços devem ser sempre garantidos, a mínima falha nas comunicações de dados ou de voz é um problema com que me deparo todos os dias.

Deste modo, observo o quanto é importante a redundância numa rede e será interessante continuar o estudo das tecnologias apresentadas nesta dissertação e aprofundar a análise em cenários onde ocorreram maiores dificuldades, como é o caso da redundância em VPNs SSL.

O melhoramento de tempos de resposta na alternância entre ligações redundantes é também uma boa opção para um estudo futuro.

Referências Bibliográficas

[1] Stalling, W., “Data and Computer Communications”, Prentice Hall, 1999;

[2] Comer, D., “Internetworking with TCP/IP”, Prentice Hall, 2006;

[3] Leon-Garcia, A., “Communication Networks”, Mc Graw Hill, 2004;

[4] Peterson, L., “Computer Networks”, Morgan Kaufmann, 2007;

[5] McCabe, J., “Network Analysis, Architecture, and Design”, Morgan Kaufmann, 2007;

[6] Zuquete, A., “Segurança em Redes Informáticas”, FCA, 2008;

[7] Snader, J., “VNPs Ilustrated Tunnels, VPNs, and IPSec”, Addison Wesley, 2005;

[8] Bollapragada, V., “IPSec VPN Design”, Cisco Press, 2005;

[9] Dierks, T., “The Transport Layer Security (TLS) Protocol”, version 1.1, RFC 4346, IETF, Abril 2006;

[10] Kent, S., “Security Architecture for the Internet Protocol, RFC2401, IETF, Novembro 1998;

[11] Nedeltchev, P., “Troubleshooting Remote Access Networks”, Cisco Press, 2002;

[12] Manuel da Cisco, “Cisco Network-Based IPSec VPN Solucion Release 1.5 Operations, Maintenance, and Troubleshooting Guide” (versão em pdf), 2003;

[13] Manual da Cisco, “Cisco Secure VPN Client Solutions Guide” (versão em pdf), 1999;

[14] Manual da Cisco, “Cisco PIX Firewall and VPN Configuration Guide” (versão em pdf), 2003;

[15] Deal, D., “The Complete Cisco VPN Configuration Guide”, Cisco Press, 2006;

[16] Neumann, J., “Cisco Routers for the Small Business”, Apress, 2009;

[17] Carmouche, J., “IPSec Virtual Private Network Fundamentals”, Cisco Press, 2006;

[18] Frahim, J., “SSL Remote Access VPNs”, Paperback, 2008;

[19] Lewis, M., “Comparing, Designing, and Deploying VPNs”, Paperback, 2006;

[20] Mairs, J., “VPNs: A Beginner's Guide”, Paperback, 2001;

[21] Manual da Cisco. Disponível em http://www.cisco.com/web/PT/empresas/st/vpn/index.html. Último acesso em 15-11-2009;

[22] Manual da Check Point. Disponível em http://www.checkpoint.com/products/softwareblades/ipsec-virtual-private-network.html. Último acesso em 15-11-2009;

[23] Manual da Juniper. Disponível em http://www.juniper.net/us/en/local/pdf/brochures/1500024-en.pdf. Último acesso em 15-11-2009;

[24] Manual da Citrix. Disponível em http://www.citrix.com/English/PS2/products/product.asp?contentID=15005. Último acesso em 15-11-2009;

[25] Manual da Fortinet. Disponível em http://www.fortinet.com/solutions/vpn.html. Último acesso em 15-11-2009;

[26] Manual da Dlink. Disponível em http://www.dlink.com/category/productcategories/?cid=79. Último acesso em 15-11-2009;

[27] VRRP – http://blog.ccna.com.br/2008/12/16/pr-vrrp-x-hsrp-x-glbp/. Último acesso em 11-01-2010;

[28] VRRP – http://wiki.mikrotik.com/wiki/VRRP. Último acesso em 09-01-2010;

[29] Cisco VPN Client – http://www.cisco.com/en/US/products/sw/secursw/ps2308/prod_configuration_examples_list.html. Último acesso em 11-01-2010;

[30] Cisco SSL VPN – http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html - Último acesso em 23-12-2009;

[31] Cisco Web VPN – http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008071c58b.shtml. Último acesso em 11-12-2009;

[32] OpenVPN – http://openvpn.net/. Último acesso em 17-12-2009;

[33] VPNC – http://www.vpnc.org/. Último acesso em 19-01-2010;

Anexos

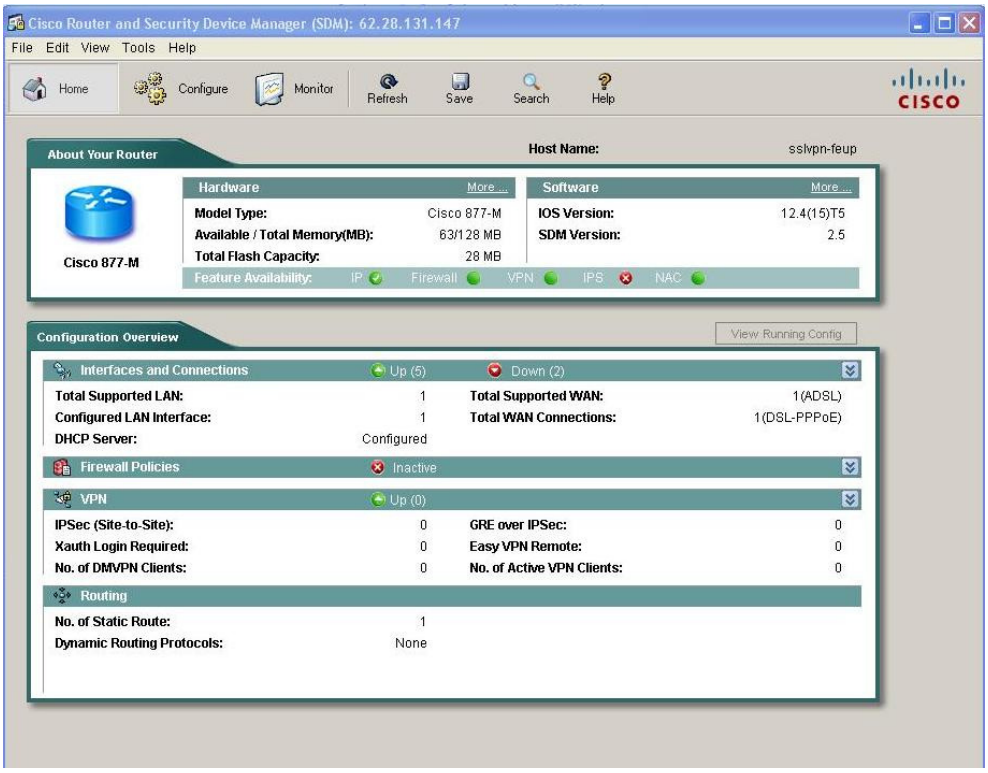
Anexo A

```
hostname sslvpn-feup
clock set 18:34:00 9 Dec 2009

! configurar o DHCP para a LAN, excluindo o 192.168.1.1 porque será atribuído
à LAN
! Os IPs 62.48.131.10 62.48.131.11 são os ips de DNS

no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1
ip dhcp pool DHCP_LAN
   import all

   network 192.168.1.0 255.255.255.0
   dns-server 62.48.131.10 62.48.131.11
   default-router 192.168.1.1
   lease 0 1

ip domain name sslvpn-feup
username alima privilege 15 secret 5 $1$JPif$JQbHI3z/d9IsCd/W4eW9K.

! interface virtual sempre a responder

interface Loopback0
 ip address 10.1.1.1 255.255.255.255

! configuração do acesso adsl

interface ATM0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
interface ATM0.1 point-to-point
 description -=- DSL79792 - 226001914 -=-
 pvc 0/35
  pppoe max-sessions 1
  pppoe-client dial-pool-number 1

! configuração da rede local

interface Vlan1
 description -=- LAN -=-
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
```

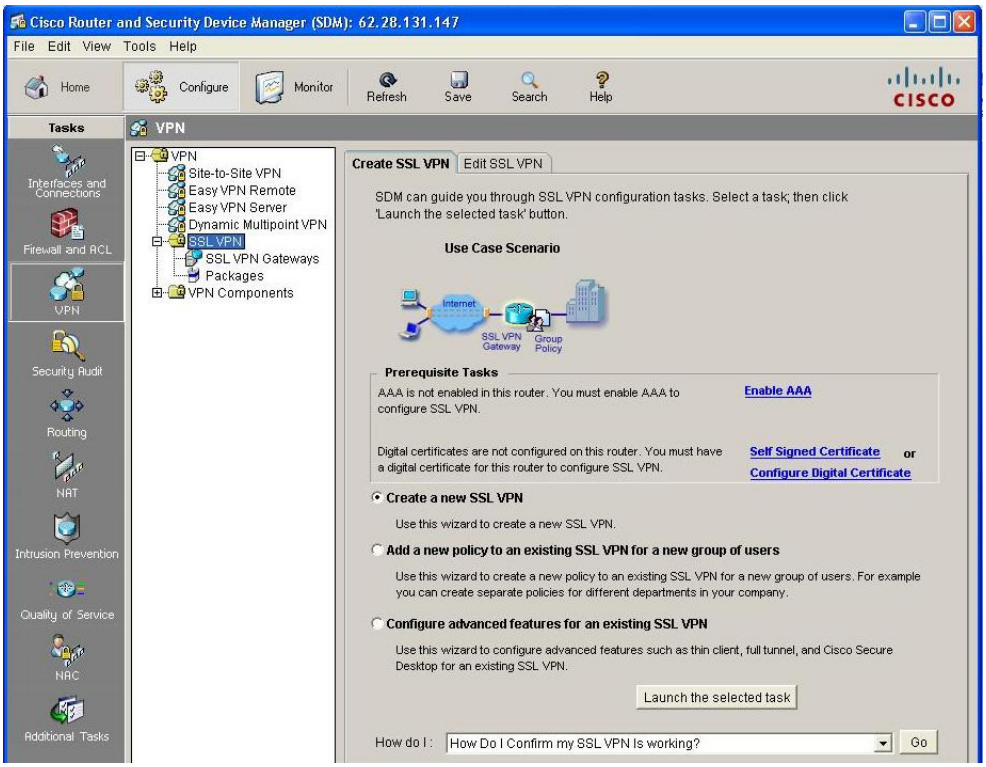
```
! conta ADSL

interface Dialer1
 description -=- Saida para Internet 62.28.131.147 -=-
 ip address negotiated
 no ip unreachables
 ip mtu 1492
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 dialer pool 1
 dialer idle-timeout 0
 dialer-group 1
 ppp pap sent-username ****@**** password 0 ****

! rota estática a apontar para a saída

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Dialer1
ip nat inside source list 70 interface Dialer1 overload

access-list 70 remark == ACL para NAT ==
access-list 70 permit 192.168.1.0 0.0.0.255
dialer-list 1 protocol ip permit

line vty 0 4
 exec-timeout 60 0
 privilege level 15
 transport input telnet ssh

! para aceder ao router via browser

ip http server
ip http authentication local
ip http secure-server
```

Anexo B

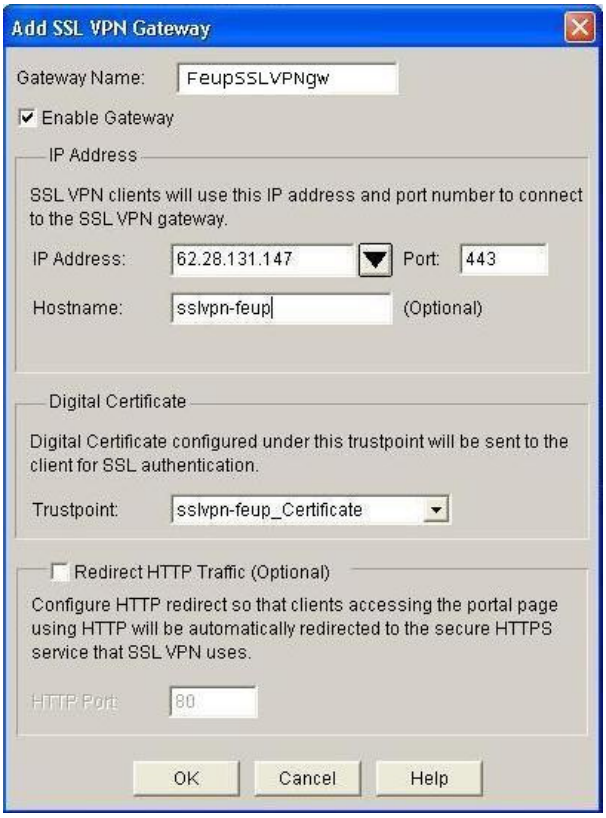
Depois de instalado o SDM no PC de testes, é também configurado o router para interagir com o SDM. Acede-se à aplicação através do IP de WAN 62.28.131.147.



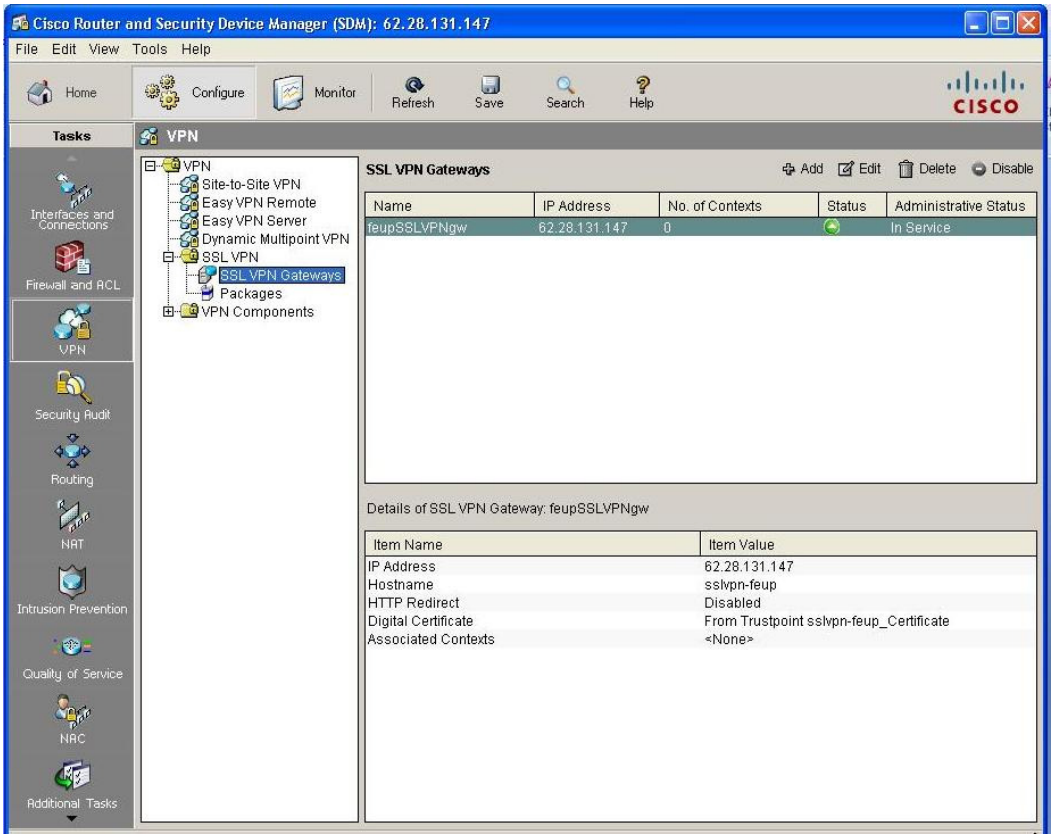
O servidor Cisco AAA e o "*self signed certificate*" são configurados. Posteriormente define-se a VPN SSL.



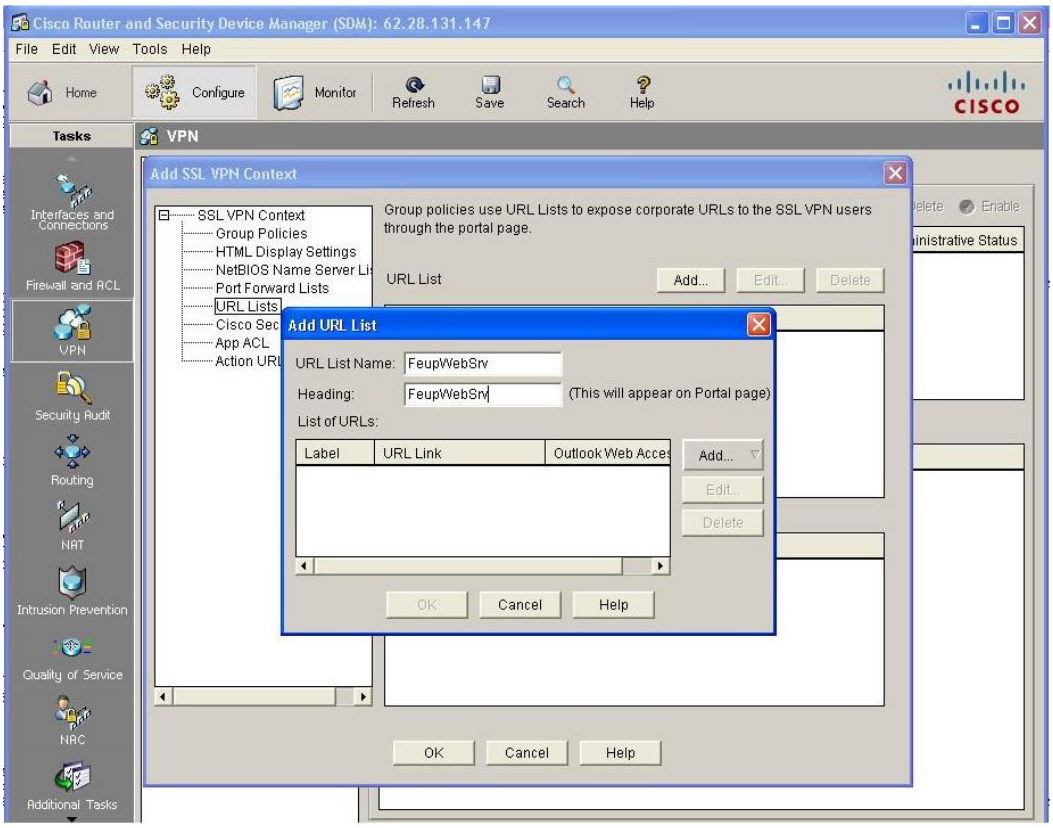
Adiciona-se uma SSL VPN *Gateway*.



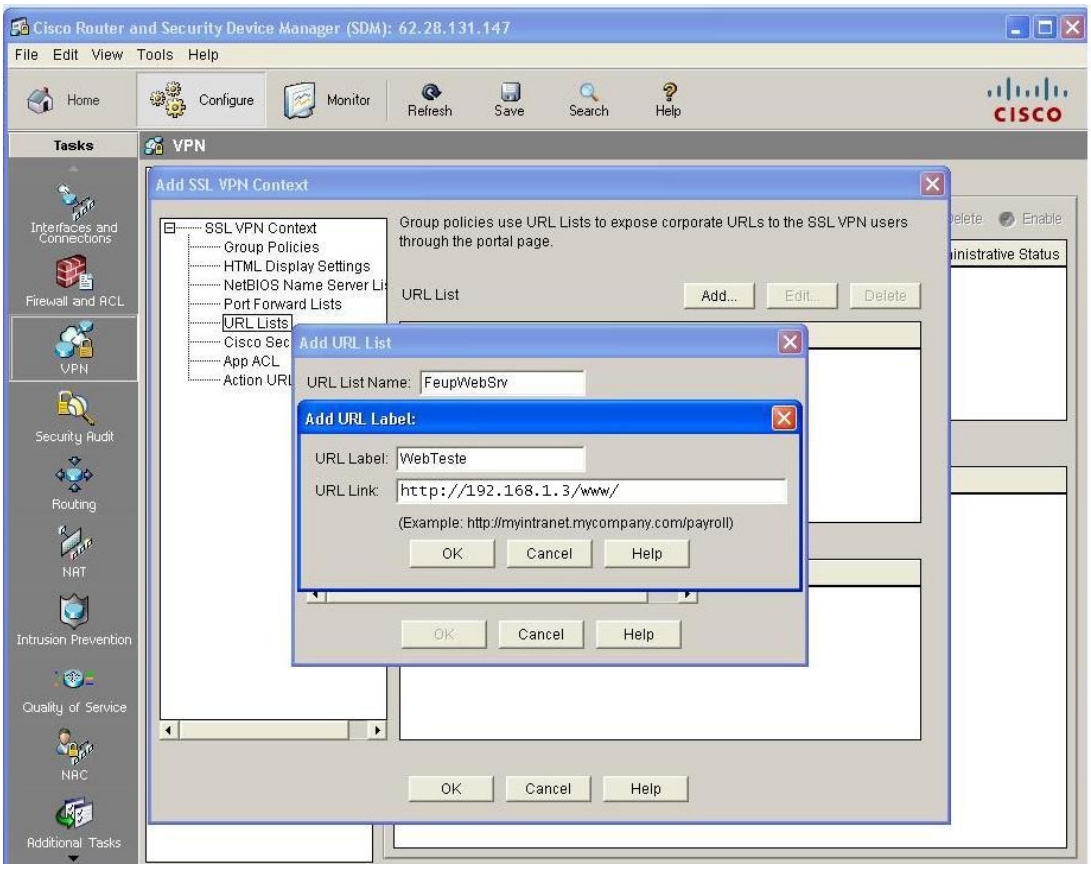
Depois de introduzidos os campos, as alterações são assumidas.



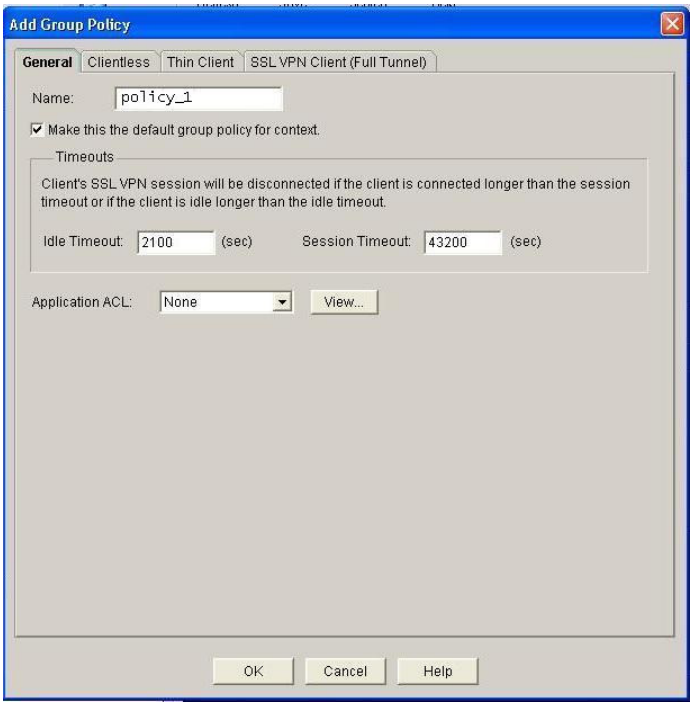
De forma a facilitar a introdução de recursos ao grupo de politicas, pode-se configurar os recursos antes da criação do grupo de politicas. Cria-se a *WebVPN Context*.



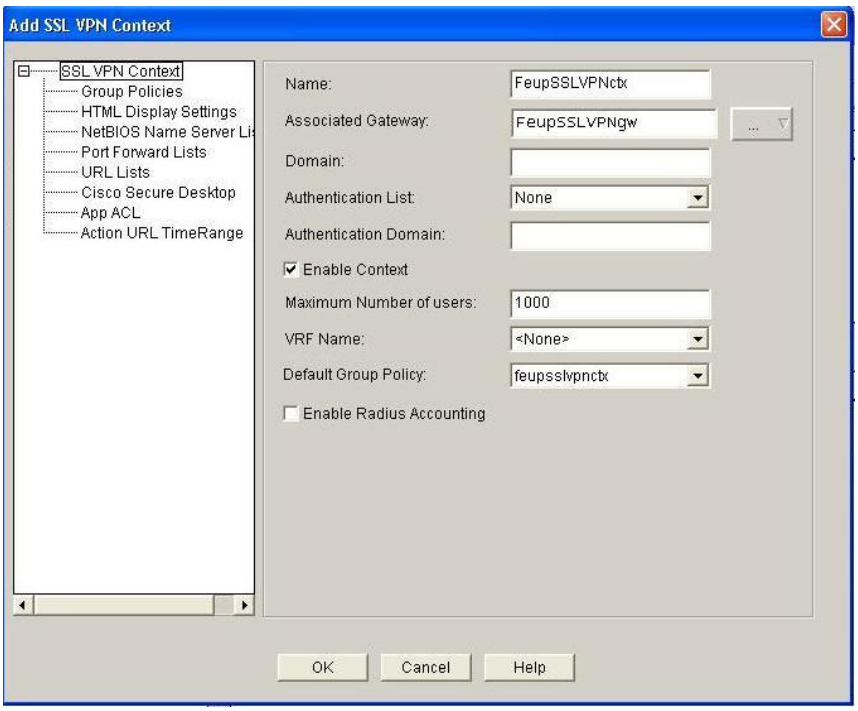
Depois de se adicionar a URL *Lists*, insere-se o nome e cabeçalho da URL, escolhendo *Website*.



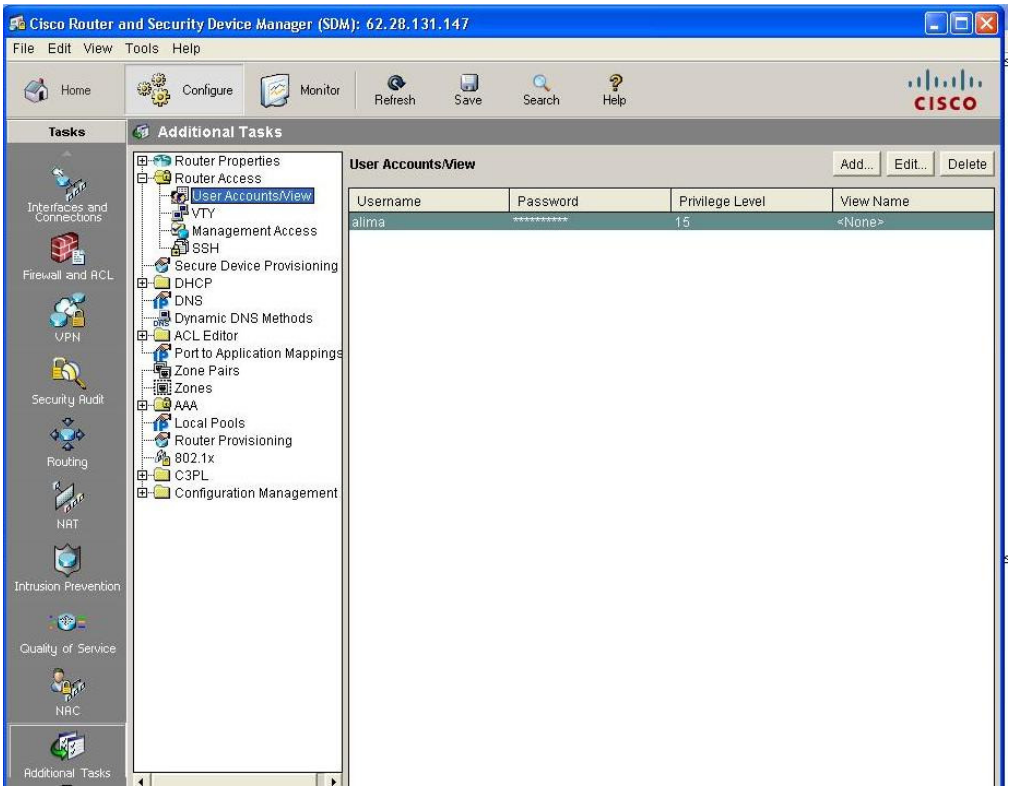
Esta lista contém todos os servidores *web* (HTTP e HTTPS), que se tornaram disponíveis aos utilizadores remotos. O recurso do acesso a ficheiros através do CIFS (*Windows file browsing*) está disponível, designado um servidor de NetBIOS (NBNS), com o IP 192.168.1.10. Adiciona-se agora a *Group Policy*:



Clica-se no marcador *Clientless* e coloca-se um visto em *Select* para a URL *List* escolhida. De modo a interligar a *gateway WebVPN*, a politica de grupo e os recursos disponíveis, configura-se um contexto *WebVPN*. Escolhe-se *WebVPN Context* e insere-se o nome "FeupSSLVPNctx", e clica-se na lista *Associated Gateway* e escolhe-se a *gateway* pretendida "FeupSSLVPNgw".



Clica-se em *Configuration*, e de seguida em *Additional Tasks*. Abre-se o *Router Access*, e escolhe-se *User Accounts/View*. Como se pode ver, o *user* alima já está criado com o máximo de privilégios.



Depois de todos estes passos, o router gera a configuração que está no Anexo C.

Anexo C

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sslvpn-feup
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
aaa session-id common
!
crypto pki trustpoint sslvpn-feup_Certificate
 enrollment selfsigned
 serial-number none
 ip-address none
 revocation-check crl
 rsakeypair sslvpn-feup_Certificate_RSAKey 512
!
! Informação do certificado gerado automaticamente

crypto pki certificate chain sslvpn-feup_Certificate
 certificate self-signed 01
  308201B8 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  28312630 2406092A 864886F7 0D010902 16177373 6C76706E 2D666575 702E7373
  6C76706E 2D666575 70301E17 0D303931 32303932 31303735 345A170D 32303031
  30313030 30303030 5A302831 26302406 092A8648 86F70D01 09021617 73736C76
  706E2D66 6575702E 73736C76 706E2D66 65757030 5C300D06 092A8648 86F70D01
  01010500 034B0030 48024100 DCCF38F8 0516BF95 101A99D4 BB71C24E EBC5BFBD
  837A91A2 60E2F2BE 71A1B9D8 9F72B527 37CEACB1 2D85A5F5 93ED02DB 3623D8ED
  D86C3181 44B1ED0F 30E6AE1D 02030100 01A37730 75300F06 03551D13 0101FF04
  05300301 01FF3022 0603551D 11041B30 19821773 736C7670 6E2D6665 75702E73
  736C7670 6E2D6665 7570301F 0603551D 23041830 168014C4 BCC7B35F 3D7F0969
  33FBB930 62A55335 62C6A430 1D060355 1D0E0416 0414C4BC C7B35F3D 7F096933
  FBB93062 A5533562 C6A4300D 06092A86 4886F70D 01010405 00034100 305DF8B9
  4186EE3D 669C7D7C 1FD097DD C1A67FFB 217567A3 2BB4AB1C 831F41EE E864CA91
  4475AF7C 1970391F 69C4F6C6 4F0E37D5 A80ED253 B33DBFBF 916AAAA5
        quit
dot11 syslog
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1
!
ip dhcp pool DHCP_LAN
   import all
   network 192.168.1.0 255.255.255.0
   dns-server 62.48.131.10 62.48.131.11
   default-router 192.168.1.1
   lease 0 1
!
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ip domain name sslvpn-feup
!
```

```
!
vtp mode transparent
username alima privilege 15 secret 5 $1$JPif$JQbHI3z/d9IsCd/W4eW9K.
!
!
archive
 log config
  hidekeys
!
vlan 10
!
ip ssh version 1
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
interface ATM0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.1 point-to-point
 description -=- DSL79792 - 226001914 -=-
 pvc 0/35
  pppoe max-sessions 1
  pppoe-client dial-pool-number 1
 !
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 description -=- LAN -=-
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Vlan2
 no ip address
!
interface Dialer1
 description -=- Saida para Internet 62.28.131.147 -=-
 ip address negotiated
 no ip unreachables
 ip mtu 1492
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 dialer pool 1
 dialer idle-timeout 0
 dialer-group 1
 ppp pap sent-username ****@**** password 0 *****
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Dialer1
!
ip http server
ip http authentication local
ip http secure-server
```

```
ip nat inside source list 70 interface Dialer1 overload
!
access-list 70 remark == ACL para NAT ==
access-list 70 permit 192.168.1.0 0.0.0.255
dialer-list 1 protocol ip permit
!
control-plane
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 exec-timeout 60 0
 privilege level 15
 transport input telnet ssh
!
scheduler max-task-time 5000
!
! Gateway WebVPN

webvpn gateway FeupSSLVPNgw
 hostname sslvpn-feup
 ip address 62.28.131.147 port 443
 http-redirect port 80
 ssl trustpoint sslvpn-feup_Certificate
 inservice
 !
webvpn context FeupSSLVPNctx
 ssl authenticate verify all

! Identify resources for the SSL VPN session

 url-list "FeupWebSrv"
   heading "FeupWebTest"
   url-text "WebTest" url-value "http://192.168.1.3/www/"
 !
 nbns-list "NBNSServers"
   nbns-server 192.168.1.10
 !
! Identificação da politica de grupo que controlará os recursos existentes

 policy group policy_1
   url-list "FeupWebSrv"
   nbns-list "NBNSServers"
   functions file-access
   functions file-browse
   functions file-entry
   hide-url-bar
   citrix enabled
 default-group-policy policy_1
 gateway FeupSSLVPNgw
 max-users 2
 inservice
!
end
```

Anexo D

Configurações **Router A**:

```
! Configuração da politica de IKE no router (1ª Fase)
! Tipo de encriptação e hash – DES e SHA por defeito
! O tipo de chave utilizada – pre-share (chave01 e chave02 serão as chaves utilizadas)
! Os IPs 10.1.1.2 e 10.2.2.2 são a identificação dos extremos das VPNs

crypto isakmp policy 1000
 authentication pre-share
 lifetime 84600
crypto isakmp key chave01 address 10.1.1.2
crypto isakmp key chave02 address 10.2.2.2

! Configuração do IPSec (2ª Fase)
! Transform-set AH
! Encriptação ESP

crypto ipsec transform-set vpnipsec ah-sha-hmac esp-des esp-sha-hmac
 mode transport

! Configuração de mapeamentos para definição dos extremos dos túneis
! As access-lists 101 e 102 apenas permitirão o estabelecimento dos túneis IPSec

crypto map ISP1 local-address Serial0/1/0
crypto map ISP1 1 ipsec-isakmp
 set peer 10.1.1.2
 set transform-set vpnipsec
 match address 101
!
crypto map ISP2 local-address FastEthernet0/1
crypto map ISP2 2 ipsec-isakmp
 set peer 10.2.2.2
 set transform-set vpnipsec
 match address 102

! Configuração dos túneis IPSec para a criação das VPNs

interface Tunnel1
 ip address 10.10.10.1 255.255.255.252
 tunnel source 10.1.1.1
 tunnel destination 10.1.1.2
 crypto map ISP1
!
interface Tunnel2
 ip address 10.20.20.1 255.255.255.252
 tunnel source 10.2.2.1
 tunnel destination 10.2.2.2
 crypto map ISP2

! Configuração da interface para a rede local

interface FastEthernet0/0
 description REDE LOCAL
 ip address 192.168.1.254 255.255.255.0

! Configuração da interface para a ligação ao ISP2

interface FastEthernet0/1
 description LIGACAO AO ISP2
 ip address 10.2.2.1 255.255.255.252
crypto map ISP2
```

```
! Configuração da interface para a ligação ao ISP1

interface Serial0/1/0
 description LIGACAO AO ISP1
 ip address 10.1.1.1 255.255.255.252
crypto map ISP1

! Configuração do protocolo de routing OSPF para divulgação das redes (deste
modo a rede local será difundida através das duas ligações redundantes)

router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/1
 passive-interface Serial0/1/0
 network 10.10.10.0 0.0.0.3 area 5
 network 10.20.20.0 0.0.0.3 area 5
 network 192.168.1.0 0.0.0.255 area 5

! Todo o tráfego que passará através do túnel (GRE) é encriptado pelo IPSec

access-list 101 permit gre host 10.1.1.1 host 10.1.1.2
access-list 102 permit gre host 10.2.2.1 host 10.2.2.2

! Se o tráfego corresponder com a ACL 101 as redes não serão difundidas e a
próxima route-map não será executada

route-map linkISP1 deny 15
 match ip address 101
!
!
route-map linkISP1 permit 25
 match interface Serial0/1/0
!
route-map linkISP2 deny 15
 match ip address 102
!
route-map linkISP2 permit 25
 match interface FastEthernet0/1
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Configurações **Router B:**

```
! Configuração da politica de IKE no router (1ª Fase)
! Tipo de encriptação e hash - DES e SHA por defeito
! O tipo de chave utilizada - pre-share (chave01 e chave02 serão as chaves
utilizadas)
! Os IPs 10.1.1.1 e 10.2.2.1 são a identificação dos extremos das VPNs

crypto isakmp policy 1000
 authentication pre-share
 lifetime 84600
crypto isakmp key chave01 address 10.1.1.1
crypto isakmp key chave02 address 10.2.2.1
```

```
! Configuração do IPSec (2ª Fase)
! Transform-set AH
! Encriptação ESP

crypto ipsec transform-set vpnipsec ah-sha-hmac esp-des esp-sha-hmac
 mode transport

! Configuração de mapeamentos para definição dos extremos dos túneis
! As access-lists 101 e 102 apenas permitirão o estabelecimento dos túneis
IPSec

crypto map ISP1 local-address Serial0/0/0
crypto map ISP1 1 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set vpnipsec
 match address 101
!
crypto map ISP2 local-address FastEthernet0/1
crypto map ISP2 2 ipsec-isakmp
 set peer 10.2.2.1
 set transform-set vpnipsec
 match address 102

! Configuração dos túneis IPSec para a criação das VPNs

interface Tunnel1
 ip address 10.10.10.2 255.255.255.252
 tunnel source 10.1.1.2
 tunnel destination 10.1.1.1
 crypto map ISP1
!
interface Tunnel2
 ip address 10.20.20.2 255.255.255.252
 tunnel source 10.2.2.2
 tunnel destination 10.2.2.1
 crypto map ISP2

! Configuração da interface para a rede local

interface FastEthernet0/0
 description REDE LOCAL
 ip address 192.168.2.254 255.255.255.0

! Configuração da interface para a ligação ao ISP2

interface FastEthernet0/1
 description LIGACAO AO ISP2
 ip address 10.2.2.2 255.255.255.252
crypto map ISP2

! Configuração da interface para a ligação ao ISP1

interface Serial0/0/0
 description LIGACAO AO ISP1
 ip address 10.1.1.2 255.255.255.252
crypto map ISP1

! Configuração do protocolo de routing OSPF para divulgação das redes (deste
modo a rede local será difundida através das duas ligações redundantes)

router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/1
 passive-interface Serial0/0/0
 network 10.10.10.0 0.0.0.3 area 5
 network 10.20.20.0 0.0.0.3 area 5
 network 192.168.2.0 0.0.0.255 area 5
```

```
! Todo o tráfego que passará através do túnel (GRE) é encriptado pelo IPSec

access-list 101 permit gre host 10.1.1.2 host 10.1.1.1
access-list 102 permit gre host 10.2.2.2 host 10.2.2.1

! Se o tráfego corresponder com a ACL 101 as redes não serão difundidas e a
próxima route-map não será executada

route-map linkISP1 deny 15
 match ip address 101
!
!
route-map linkISP1 permit 25
 match interface Serial0/0/0
!
route-map linkISP2 deny 15
 match ip address 102
!
route-map linkISP2 permit 25
 match interface FastEthernet0/1
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Anexo E

Configurações **Router B**:

```
! Configuração da politica de IKE no router (1ª Fase)
! Tipo de encriptação e hash – DES e SHA por defeito
! O tipo de chave utilizada – pre-share (chave01)
! O IP 10.1.1.1 é a identificação do extremo da VPN (túnel)

crypto isakmp policy 1000
 authentication pre-share
 lifetime 84600
crypto isakmp key chave01 address 10.1.1.1

! Configuração do IPSec (2ª Fase)
! Transform-set AH
! Encriptação ESP

crypto ipsec transform-set vpnipsec ah-sha-hmac esp-des esp-sha-hmac
 mode transport

! Configuração do mapeamento para definição dos extremos dos túneis
! A access-list 101 apenas permite o estabelecimento do túnel IPSec

crypto map ISP1 local-address Serial0/0/0
crypto map ISP1 1 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set vpnipsec
 match address 101

! Configuração do túnel IPSec para a criação da VPN

interface Tunnel1
 ip address 10.10.10.2 255.255.255.252
 tunnel source 10.1.1.2
 tunnel destination 10.1.1.1
 crypto map ISP1

! Configuração da interface para a rede local com os parâmetros de VRRP – este
equipamento ficará o Master devido a ter uma prioridade mais alta, o tempo de
divulgação é de 3 segundos

interface FastEthernet0/0
 description REDE LOCAL
 ip address 192.168.2.253 255.255.255.0
 vrrp 1 priority 120
 vrrp 1 192.168.2.254
 vrrp 1 timers advertise 3

! Configuração da interface para a ligação ao ISP1

interface Serial0/0/0
 description LIGACAO AO ISP1
 ip address 10.1.1.2 255.255.255.252
 crypto map ISP1

! Configuração do protocolo de routing OSPF para divulgação das redes (deste
modo a rede local será difundida através da ligação)

router ospf 1
 log-adjacency-changes
 passive-interface Serial0/0/0
 network 10.10.10.0 0.0.0.3 area 5
 network 192.168.2.0 0.0.0.255 area 5

! Todo o tráfego que passará através do túnel (GRE) é encriptado pelo IPSec

access-list 101 permit gre host 10.1.1.2 host 10.1.1.1
```

```
! Se o tráfego corresponder com a ACL 101 as redes não serão difundidas e a
próxima route-map não será executada

route-map linkISP1 deny 15
 match ip address 101
!
route-map linkISP1 permit 25
 match interface Serial0/0/0
```

Configurações **Router C**:

```
! Configuração da politica de IKE no router (1ª Fase)
! Tipo de encriptação e hash – DES e SHA por defeito
! O tipo de chave utilizada – pre-share (chave02)
! O IP 10.2.2.1 é a identificação do extremo da VPN (túnel)

crypto isakmp policy 1000
 authentication pre-share
 lifetime 84600
crypto isakmp key chave02 address 10.2.2.1

! Configuração do IPSec (2ª Fase)
! Transform-set AH
! Encriptação ESP

crypto ipsec transform-set vpnipsec ah-sha-hmac esp-des esp-sha-hmac
 mode transport

! Configuração do mapeamento para definição do extremo dos túnel
! A access-list 102 apenas permite o estabelecimento do túnel IPSec

crypto map ISP2 local-address FastEthernet0/1
crypto map ISP2 2 ipsec-isakmp
 set peer 10.2.2.1
 set transform-set vpnipsec
 match address 102

! Configuração do túnel IPSec para a criação da VPN

interface Tunnel2
 ip address 10.20.20.2 255.255.255.252
 tunnel source 10.2.2.2
 tunnel destination 10.2.2.1
 crypto map ISP2

! Configuração da interface para a rede local com os parâmetros de VRRP – este
equipamento ficará como Slave devido a ter a prioridade por defeito (100)

interface FastEthernet0/0
 description REDE LOCAL
 ip address 192.168.2.252 255.255.255.0
 vrrp 1 192.168.2.254
 vrrp 1 timers advertise 3

! Configuração da interface para a ligação ao ISP2

interface FastEthernet0/1
 description LIGACAO AO ISP2
 ip address 10.2.2.2 255.255.255.252
 crypto map ISP2

! Configuração do protocolo de routing OSPF para divulgação das redes

router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/1
 network 10.20.20.0 0.0.0.3 area 5
 network 192.168.2.0 0.0.0.255 area 5
```

```
! Todo o tráfego que passará através do túnel (GRE) é encriptado pelo IPSec

access-list 102 permit gre host 10.2.2.2 host 10.2.2.1

! Se o tráfego corresponder com a ACL 102, as redes não serão difundidas e a
próxima route-map não será executada

route-map linkISP2 deny 15
 match ip address 102
!
route-map linkISP2 permit 25
 match interface FastEthernet0/1
```