UNIVERSIDADE DE TAUBATÉ
Pedro Celestino

REDES VIRTUAIS PRIVADAS

Taubaté – SP

2005

UNIVERSIDADE DE TAUBATÉ
Pedro Celestino

REDES VIRTUAIS PRIVADAS

Dissertação apresentada para obtenção do Título de Mestre em Automação do Departamento de Pós Graduação em Engenharia Mecânica da Universidade de Taubaté.

Área de Concentração: Automação Industrial e Robótica

Professor Orientador: Prof. *Dr. Luiz Octávio Mattos dos Reis*

Taubaté – SP
2005

Pedro Celestino

Título: Redes Virtuais Privadas

Universidade de Taubaté, Taubaté, SP

Data : 03/12/2005.

Resultado_____

Banca Examinadora

Prof.Dr. _____ Instituição_____

Assinatura _____

Prof.Dr. _____ Instituição_____

Assinatura _____

Prof.Dr. _____ Instituição_____

Assinatura _____

Prof.Dr. _____ Instituição_____

Assinatura _____

Prof.Dr. _____ Instituição_____

Assinatura _____

Dedico este trabalho ao meu orientador Prof. Dr.Luiz Octavio Mattos dos Reis, pelo incentivo conferido ao meu trabalho durante sua pesquisa e execução.

Aos meus queridos pais (in memorian), com a certeza de estarem orgulhosos por mais esse patamar alcançado e agradecendo a eles tudo o que sou e que tenho hoje. Aos meus filhos Flávio, Ricardo e Fernanda, que sirva como exemplo de vida, objetivando a realização

CELESTINO, Pedro.
U17p Redes Virtuais Privadas./ Celestino Pedro. – Taubaté: Unitau, 2005.

89 f. il; 30 cm.

Dissertação (Mestrado) – Universidade de Taubaté. Departamento de Engenharia Mecânica. 2005
Orientador: Prof. Dr. Luiz Octávio Mattos dos Reis.

1.Redes Virtuais. 2.Automatização de processos
Mestrado. I. Universidade de Taubaté. Departamento de Engenharia Mecânica. II. Título.

Agradecimentos

À Professora Márcia Rejane pela ajuda nas correções e em particular a minha assistente e grande amiga Nadya Moscoso Cicarelli pela correção ortográfica.

RESUMO

Com as redes de computadores, surge também a possibilidade de administrar remotamente as organizações inteligentes, no entanto a troca de informações segura tornou-se um problema para as instituições que trafegam dados estruturados através das redes de computadores. Um dos maiores desafios é a busca de soluções economicamente viáveis e ao mesmo tempo seguras. Protocolos de segurança, algoritmos criptográficos meios de comunicação seguros, são itens essenciais para que a informação possa trafegar em ambientes livres de interferências externas. Uma das soluções é a Rede Virtual Privada. Neste trabalho, serão apresentados os principais destaques desta tecnologia, utilizando o protocolo IPSec, com o propósito de apresentar mais uma solução atrativa para as organizações, pois trata-se de uma solução economicamente viável e segura.

PALAVRAS- CHAVES: Redes de Computadores, Segurança em Redes, Criptografia, IPSec, Windows

Celestino, Pedro. **REDES VIRTUAIS PRIVADAS**. 2005 - Dissertação de Mestrado em Engenharia de Automação – Departamento de Engenharia Mecânica – Universidade de Taubaté, Taubaté.

ABSTRACT

Along with the computers networks emerges the possibility of managing remotely the intelligent organizations although the safe change of information has become a problem to the institutions which transport structured data through nets of computers. One of the largest challenges is the search for safe and economically viable solutions. Protocols of safety, cryptographic algorithms, safe means of communication are essential items so that the information can travel in environmentals free of external interferences. One of the alternatives is the Virtual Private Networks. In this work , the main prominences of this technology will be presented using the protocol IPSec with the purpose of presenting a more atractive tool to the organizations due to its safety and economical viability.

KEY WORDS: Computers Networks, Security in Networks, Cryptography,Windows.

Celestino, Pedro. PRIVATE VIRTUAL NETWORK. 2005 - dissertation of Mestrado in Engineering of Automation - Department of Mechanical Engineering - University of Taubaté, Taubaté

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

Sigla	Significado da sigla
AES	Advanced Encryption Standard – padrão de encriptação
AH	Authentication Header – Cabeçalho de autenticação
ARPANET	Advanced Research Projects Agency Network
AS	Security Association – AS – Associação segura
ATM	Asynchronous Transfer Mode – Modo de transferência assíncrono
CAST	Carlisle Adams and Stafford Tavares
DAS	Dual Attachment Station – Estação de anexo dual
DES	Data Encryption Standard – Encriptação padrão de dados
DoS	Denial of Service – Negação ao Serviço
DSL	Digital Subscriber Line – Subscritor de linha digital
ESP	Encapsulating Security Payload – Encapsulamento de Segurança
FTP	File Transfer Protocol – Protocolo deTransferência de arquivos
ICP	Internet Control Protocol – Protocolo de controle da internet
IETF	Internet Engineering Task Force – Força tarefa de engenharia
IKE	Internet Key Exchange – Chave de troca da Internet
IP	Internet Protocol – Protocolo de Internet
IPSec	Internet Protocol Security – Protocolo de internet Seguro
IPX/SPX	Interwork Packet Exchange / Sequenced Packet Exchange
ISP	Internet Service Provider – Provedor de serviço de internet
ITU-T	International Telecomunication Union – Telecommunication Standardization Sector – União Internacional de telecomunicações – Setor de Padronização de telecomunicações
L2TP	Layer Two Tunneking Protocol – Protocolo da segunda camada
LAN	Local Area Network – Rede de alcance local
MAN	Metropolitan Area Network – Rede de alcance Metroplolitano
Net Bios	Network Basic Input/Output System
NetBeui	Network Basic Input/ Output System- Extended User Interface
PAP	Password Authentication Protocol – Protocolo de autenticação
PKI	Public Key Infrastructure – Infraestrutura de chave Pública
POP	Post Office Protocol - Point of Presence – Ponto de Presença
PPP	Point-to-point Protocol – Protocolo ponto a ponto
PPTP	Point to Point Tunnel Protocol – Protocolo Ponto a Ponto Tunelado
RADIOS	Remote Authentication Dial-In User Service – Serviço de autenticação a distância
RNP	Rede Nacional de Ensino e Pesquisa
RSA	Rivest-Shamir-Adelman -
SMTP	Simple Mail Transfer Protocol – protocolo simples de transferência de correio.
SPI	Service Provider Interface – Interface de provedor de serviço
TACACS	Terminal Access Controller Access Control System – Sistema controlador de acesso terminal
TCP/IP	Transmission Control Protocol/Internet Protocol – Protocolo de controle de transmissão / protocolo Internet
VPN	Virtual privates network – Redes Virtuais Privadas
WAN	Wide Area Network - Rede de Grande Área
MD-5	Message Digest 5 – Resumo de Mensagem 5
SHA-1	Secure Hash Algorithm – Algoritmo Hash seguro
3DES	Triple Data Encryption Standard – Encriptador triplo padrão

Lista de Figuras

Lista de Tabela

REFERÊNCIAS BIBLIOGRÁFICAS

BASTOS,Eri Ramos. Configurando uma VPN IPSec FreeSwan no Linux. [S.l.], 2002. Disponível em: http://www.secforum.com.br/article.php?sid=1033>.

Marcelo Duffles Donato Moreira. Função Hash e Autenticação em Redes de Computadores. 2005 Universidade Federal do Rio de Janeiro

BROCARDO, Marcelo Luiz 12AC: um Protocolo Criptográfico para Análise Segura de Crédito.2001.122 1.Dissertação de Mestrado em ciência da Computação – Universidade Federal de Santa Catarina, Florianópolis.

BROWNE: Brian el al. Best Practices For VPN Implementation. [S.l], 2001. Disponível em: http://www.bcr.com/bcrmag/2001/03/p24.asp>.

Torres Gabriel Redes de Computadores - Curso Completo. Axcel Books, 2001.

R. Yuan; W.T. Strayer. Virtual Private Networks – Techologies and Solutinos. Editora Addison-Wesley, 2001

CYCLADES. Guia Internet de Conectividade 6ª Edição: São Paulo, SENAC, 2000.
167 p.
3COM CORPORATION. 3COM OfficeConnect: Network Assistant. Santa Clara, EUA:3Com, versão 2.02,2000.

Alan Tamer Vasques e Rafael Priante Schuber : trabalho de conclusão de curso de bacharelado pela :http://www.abusar.org/tutoriais.html

Soares, Luiz Fernando Gomes, Lemos, Guido e Colcher, Sérgio. Redes de Computadores – das LANs, MANs e WANs, às Redes ATM. Rio de Janeiro, Campus, 1995.

KOLENISKOV, Oleg;HATCH, Brian, BuildingbLinux Virtual Private Networks (VPNs)-
1ª Edição. EUA: New Riders, 2002.385 p.
MODULAR Algo Support, Version 0.8.0. Desenvolvido por Juan Jose Ciarlante. [S.l.],2002. Disponível em:http://www.irrigacion.gov.ar/juanjo/ipsec>.

NAT Traversal, Version 0.4. Desenvolvido por Mathieu Lafon.[S.l.], 2002. Disponível em: http://open-source.arkoon.net/>.

X.509 Certificate Support,Version 0.9.15. Desenvolvido por Andreas Steffen.[S.l.],2002. Disponível em: <htpp://www.strongsec.com

"Virtual Private Networking: An Overview" . 29 de Maio de 1998. On-Line. http://www.microsoft.com/workshop/server/feature/vpnovw.asp. 26 de Junho de 1998.

Maughan, Douglas; Schertler, Mark; Schneider, Mark; Turner, Jeff. "Internet Security Association and Key Management Protocol (ISAKMP)". 10 de Março de 1998. On-Line. http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ISAKMP/draft-ietf-ipsec-isakmp-09.txt. 28 de Junho de 1998.

"Virtual Private Network" . 1998. On-Line. http://www.stts.com.br/vpn.htm. 28 de Junho de 1998.

"IPSEC - Internet Protocol Security". Security Project at the TCM Laboratory. On-Line. http://www.tcm.hut.fi/Tutkimus/IPSEC/ipsec.html. 20 de Junho de 1998.

Werner, José. "Tecnologias para Implantação de Redes Virtuais Privadas" . Fórum Nacional sobre Segurança de Redes e Telecomunicações. Março/1998. 20 de Junho de 1998.

SITES VISITADOS

http://www_guiadohardware_net2.htm

http://www.ent.com.br/index.asp?cod=1

http://www.cyclades.com.br/

http://www.resellerweb.com.br/

http://www.microsoft.com/mspress/prod/books/sampchap/1252.htm

http://support.microsoft.com/

http://www.cg.org.br/index.html

http://www.ciscoredacaovirtual.com/redacao/busqueda/resultados.asp?busqueda=vpn&categoria=todos

http://www.networkengines.com/sol/nsappliancеseries.aspx

http://www.portaldigitro.com.br/

http://www.abusar.org/vpn/tec.html

http://search.3com.com/search/pt_LA_AMER/query.html?qp=qp_pt_LA_AMER&col=intl3&qt=vpn

http://www.vpnc.org/vpn-technologies.html

http://www.alan.pro.br/publicacoes.htm

http://www.secforum.com.br/article.php?sid=1033

http://www.trendnet.com/po/products/TW100-BRV204_v1.htm

http://web.mit.edu/Saltzer/www/publications/protection/Basic.html

http://www.ipsec-howto.org/spanish/x161.html
http://www.telemar.com.br/id/id5.htm#vpns
http://www.homenethelp.com/vpn/