Nº do Aluno: _____Nome: _____[SRSC1920T2A001209]

Respostas à PARTE SEM CONSULTA

Questão 1)

A Assegura na pilha TCP/IP serviços de segurança suportados ao nível aplicação
B Assegura na pilha TCP/IP serviços de segurança suportados ao nível sessão
C Assegura na pilha TCP/IP serviços de segurança suportados ao nível transporte
D Assegura na pilha TCP/IP serviços de segurança suportados ao nível *Data-Link*
E Suporta Autenticação do tipo *Peer-Authentication*
F Suporta Autenticação dos pacotes (segmentos) TCP ou *datagramas* UDP
G Suporta Integridade de pacotes (segmentos) TCP ou de *datagramas* UDP
H Suporta Integridade de pacotes (*datagramas*) IPV4 ou IPv6
I Suporta Integridade de tramas (*frames*) Ethernet (LAN 802.3 ou WLAN 802.11)
J Suporta o estabelecimento de associações de segurança e *ciphersuites* com garantias de *Peer-Authentication* (dos endpoints).
K Estabelece associações de segurança e *ciphersutes* apenas válidas para fluxo unidirecional de pacotes IP
L Estabelece associações de segurança e *ciphersuites* para sessões de tráfego bidirecional entre os endpoints
M Garante confidencialidade não orientada à conexão
N Garante confidencialidade orientada à conexão
O Garante suporte para mitigação de ataques de negação de serviço
P Garante suporte de mitigação de ataques DoS por evitamento de SYN-FLOOD *Attacks* na abertura de conexões TCP
Q Utiliza no processamento do protocolo pelos *endpoints* assinaturas digitais de chave pública com verificação de certificados ou cadeias de certificados X509v3
R Só utiliza cifras simétricas, sínteses de segurança, HMACs ou CMACs
S Garante confidencialidade completa de tráfego
T Pode garantir confidencialidade parcial de tráfego
U Garante apenas pelo próprio processamento não repudiação
V Pode ser usado de forma a garantir apenas autenticação unilateral do tipo Peer-Authentication entre os endpoints

	TLS ou DTLS Handshake Protocol	*TLS ou DTLS Record Layer Protocol*	*TLS ou DTLS Change Cipher Spec. Protocol*	*TLS ou DTLS Alert Protocol*	*TLS ou DTLS Heartbeat Protocol*	*IPSec IKE*	*IPSec AH*	*IPSec ESP-E Encryption Only*	*IPSec ESP-AE Authentication and Encryption*	*IPSec ESP-AE em modo túnel*	*IPSec ESP-AE em modo tranpsorte*
A											
B											
C											
D											
E											
F											
G											
H											
I											
J											
K											
L											
M											
N											
O											
P											
Q											
R											
S											
T											
U											
V											

Nº do Aluno: _____Nome: _____[SRSC1920T2A001209]

Questão 2)

a) O subprotocolo IPSec que deve ser usado é: _____ em modo túnel.
Justificação:

b) Em cada *endpoint* deverão ser geridas no mínimo _____ SAs
Justificação:

c) Marque ***V*** como considerar adequado.

C1	C2	C3

Justificação:

d) Com base no que indicou em a), marque ***V*** como considerar adequado

	Sim	Não	Depende
Faz sentido usar IPSec usando o protocolo AH			

Justificação:

Nº do Aluno: _____Nome: _____[SRSC1920T2A001209]

Questão 3)

a) O ataque não é possível porque

b) Essa decisão permite aumentar a segurança, uma vez que

Questão 4

Formalizão do protocolo na interação entre A e B

(Apresente um diagrama temporal com o fluxo de mensagens e clarifique em legendas as construções criptográficas que propõe na formatação das mensagens. Utilize uma notação semelhante às apresentadas nas especificações de protocolo estudados (por exemplo, Kerberos)

Questão 5

a)

b)

c)

d)

e)

Nº do Aluno: _____Nome: _____[SRSC1920T2A001209]

Questão 6)

a) A "entrada" referente ao processamento do protocolo UDP (que indica como processar datagramas UDP destinadas ao porto 500) deverá estar como BYPASS não devendo ser processada como pacotes protegidos por ESP ou AH, porque (continue a argumentação**)...**

b) O que determina o tamanho mais ou menos adequado da janela é:

Nº do Aluno: _____Nome: _____[SRSC1920T2A001209]

Questão 7)

a)

b)

c)