3

IBGE
Instituto Brasileiro de Geografia e Estatística

EDITAL Nº 03/2013

Analista de Planejamento, Gestão e Infraestrutura em Informações Geográficas e Estatísticas A I

ANÁLISE DE SISTEMAS / SUPORTE À COMUNICAÇÃO E À REDE

LEIA ATENTAMENTE AS INSTRUÇÕES ABAIXO.

01 - O candidato recebeu do fiscal o seguinte material:

a) este **CADERNO DE QUESTÕES**, com o enunciado das 70 (setenta) questões objetivas, sem repetição ou falha, com a seguinte distribuição:

LÍNGUA PORTUGUESA		LÍNGUA INGLESA		RACIOCÍNIO LÓGICO QUANTITATIVO		CONHECIMENTOS ESPECÍFICOS	
Questões	Pontuação	Questões	Pontuação	Questões	Pontuação	Questões	Pontuação
1 a 15	1,0 cada	16 a 25	0,5 cada	26 a 35	1,0 cada	36 a 70	2,0 cada
Total:30,0						Total:70,0	
Total:100,0							

b) **CARTÃO-RESPOSTA** destinado às respostas das questões objetivas formuladas na prova.

02 - O candidato deve verificar se este material está em ordem e se o seu nome e número de inscrição conferem com os que aparecem no **CARTÃO-RESPOSTA**. Caso não esteja, o fato deve ser **IMEDIATAMENTE** notificado ao fiscal.

03 - Após a conferência, o candidato deverá assinar, no espaço próprio do **CARTÃO-RESPOSTA**, com caneta esferográfica de tinta preta, fabricada em material transparente.

04 - No **CARTÃO-RESPOSTA**, a marcação das letras correspondentes às respostas certas deve ser feita cobrindo a letra e preenchendo todo o espaço compreendido pelos círculos, com **caneta esferográfica de tinta preta, fabricada em material transparente**, de forma contínua e densa. A leitura ótica do **CARTÃO-RESPOSTA** é sensível a marcas escuras, portanto, os campos de marcação devem ser preenchidos completamente, sem deixar claros.

Exemplo: Ⓐ ● Ⓒ Ⓓ Ⓔ

05 - O candidato deve ter muito cuidado com o **CARTÃO-RESPOSTA**, para não o **DOBRAR, AMASSAR ou MANCHAR**. O **CARTÃO-RESPOSTA SOMENTE** poderá ser substituído se, no ato da entrega ao candidato, já estiver danificado em suas margens superior e/ou inferior - **DELIMITADOR DE RECONHECIMENTO PARA LEITURA ÓTICA**.

06 - Para cada uma das questões objetivas, são apresentadas 5 alternativas classificadas com as letras (A), (B), (C), (D) e (E); só uma responde adequadamente ao quesito proposto. O candidato só deve assinalar **UMA RESPOSTA**: a marcação em mais de uma alternativa anula a questão, **MESMO QUE UMA DAS RESPOSTAS ESTEJA CORRETA**.

07 - As questões objetivas são identificadas pelo número que se situa acima de seu enunciado.

08 - **SERÁ ELIMINADO** deste Concurso Público o candidato que:

a) se utilizar, durante a realização da prova, de aparelhos sonoros, fonográficos, de comunicação ou de registro, eletrônicos ou não, tais como agendas, relógios não analógicos, *notebook*, transmissor de dados e mensagens, máquina fotográfica, telefones celulares, *pagers*, microcomputadores portáteis e/ou similares;

b) se ausentar da sala em que se realiza a prova levando consigo o **CADERNO DE QUESTÕES** e/ou o **CARTÃO-RESPOSTA**;

c) se recusar a entregar o **CADERNO DE QUESTÕES** e/ou o **CARTÃO-RESPOSTA**, quando terminar o tempo estabelecido;

d) não assinar a **LISTA DE PRESENÇA** e/ou o **CARTÃO-RESPOSTA.**

Obs. O candidato só poderá ausentar-se do recinto da prova após **1 (uma) hora** contada a partir do efetivo início da mesma. Por motivos de segurança, o candidato **NÃO PODERÁ LEVAR O CADERNO DE QUESTÕES**, a qualquer momento.

09 - O candidato deve reservar os 30 (trinta) minutos finais para marcar seu **CARTÃO-RESPOSTA**. Os rascunhos e as marcações assinaladas no **CADERNO DE QUESTÕES NÃO SERÃO LEVADOS EM CONTA**.

10 - O candidato deve, ao terminar a prova, entregar ao fiscal o **CADERNO DE QUESTÕES** e o **CARTÃO-RESPOSTA** e **ASSINAR A LISTA DE PRESENÇA.**

11 - **O TEMPO DISPONÍVEL PARA ESTA PROVA DE QUESTÕES OBJETIVAS É DE 4 (QUATRO) HORAS,** já incluído o tempo para marcação do seu **CARTÃO-RESPOSTA**, findo o qual o candidato deverá, obrigatoriamente, entregar o **CARTÃO-RESPOSTA** e o **CADERNO DE QUESTÕES**.

12 - As questões e os gabaritos da Prova Objetiva serão divulgados no primeiro dia útil após sua realização, no endereço eletrônico da **FUNDAÇÃO CESGRANRIO (http://www.cesgranrio.org.br)**.

FUNDAÇÃO CESGRANRIO

CONHECIMENTOS ESPECÍFICOS

36

Uma empresa de serviços foi contratada para montar um equipamento de segurança que também melhore a performance de acesso a internet. Esse equipamento deve mascarar os endereços locais da rede, utilizar duas placas de rede e ser usado como cache de conteúdo web.

O equipamento a ser montado por essa empresa é um

(A) servidor honeypot
(B) servidor proxy
(C) sistema de prevenção de invasão
(D) sniffer de rede
(E) switch camada 2

37

Em uma empresa, instalou-se um sistema de certificado digital baseado em uma infraestrutura de chave pública. Ao configurar uma autoridade certificadora (AC) de uma hierarquia de certificação, houve um problema de relacionamento entre uma entidade e a sua chave pública, embutida no certificado, pois a mesma apresentou incorreções, visto que, no caso, houve uma mudança do nome do emissor.

Uma forma válida de se resolver essa situação seria fazer esse certificado ser

(A) reemitido
(B) redistribuído
(C) recombinado
(D) renomeado
(E) revogado

38

Um administrador de rede verificou a existência de constantes ataques onde havia recebimento de pacotes com endereços de origem falsos. Tais ataques ocorriam ou através de troca de IPs ou com IPs falsos acrescentados de informações de rotas enviadas junto ao pacote, de modo que, mesmo com endereço falso, as respostas iam para o hacker que executou o ataque.

Esse administrador deve montar uma defesa de forma a

(A) filtrar pacotes integrantes do protocolo IP que são utilizados para fornecer relatórios de erros à fonte original.
(B) proteger o acesso aos servidores existentes nessa rede que resolvam nomes em endereços IPs.
(C) limitar as tentativas de acesso, bloqueando um usuário se ele ultrapassar o número de tentativas de log.
(D) tornar randômica a sequência inicial dos pacotes para dificultar o ataque e o direcionamento das respostas.
(E) usar o comando “netstat” para monitorar as sessões e o tráfego de alto nível na rede interna.

39

Um firewall simples foi montado em uma empresa de comércio eletrônico para prevenir e bloquear ataques. Contudo, observou-se que vários ataques aconteceram.

Um tipo de ataque existente que o uso do firewall **NÃO** consegue evitar é um(a)

(A) acesso a sites externos que pertençam à lista interna de negação de acesso.
(B) hacker qualquer tentando fazer scan de várias portas da rede externa.
(C) pacote TCP externo marcado com um indicador SYN.
(D) transmissão de dados via rede, originados de sites ou locais externos.
(E) modificação de código do site por usuário interno para permitir SQL injection.

40

O padrão da arquitetura TCP/IP para gerenciamento de rede é o SNMP (Simple Network Management Protocol).

As regras usadas para definir e identificar as informações de gerenciamento são especificadas pelo padrão SMI (Structure of Management Information) que determina a descrição das bases de informação de gerenciamento (MIB – Management Information Base) com

(A) ASN.1
(B) SQL
(C) XML
(D) HTML
(E) XDR

41

Um remetente pode proteger o sigilo de uma mensagem em texto plano, criptografando-a com uma chave simétrica e um algoritmo de criptografia simétrica. Para enviar a chave simétrica com segurança para o destinatário, o remetente deve criptografar essa chave com um algoritmo de criptografia assimétrica e a

(A) sua chave privada
(B) sua chave pública
(C) chave privada do destinatário
(D) chave pública do destinatário
(E) própria chave simétrica

42

Os códigos maliciosos estão cada vez mais aprimorados, o que aumenta o grau de insegurança. Quando esses códigos visam a sobrecarregar os sistemas de computadores em rede com uma carga extra de tráfego de rede, para provocar um ataque de Denial of Service (DoS), são chamados

(A) trojan horses
(B) worms
(C) exploits
(D) flooders
(E) injectors

43

Uma entidade P precisa fazer várias verificações para validar um certificado digital de uma entidade Q emitido por uma Autoridade Certificadora (AC). Uma verificação das mais importantes visa à integridade e à autenticidade do certificado digital da entidade Q. Para isso, a entidade P precisa ter

(A) a chave privada da AC que emitiu o certificado digital da entidade Q.
(B) o certificado digital da AC que emitiu o certificado digital da entidade Q.
(C) a chave privada e a lista de certificados revogados da AC que emitiu o certificado digital da entidade Q.
(D) a chave pública da entidade Q e a lista de certificados revogados da AC que emitiu o certificado digital da entidade Q.
(E) a chave pública da entidade Q e a chave privada da AC que emitiu o certificado digital da entidade Q.

44

Considere um sistema de array de discos no qual se utilizam 7 discos (D1 a D7) em paralelo. Os 4 primeiros discos (D1 a D4) são usados para realizar o striping dos dados (o primeiro bit de informação no primeiro disco, segundo bit no segundo disco, e assim por diante). Os três discos restantes são utilizados para armazenar bits de paridade (3 bits – um bit em cada disco, para cada sequência de 4 bits nos discos D1 a D4) em um esquema de correção de erros semelhante ao utilizado em blocos de memória.

Esse esquema descrito corresponde a um RAID de nível

(A) 0
(B) 1
(C) 2
(D) 3
(E) 4

45

Segundo a Norma NBR ISO/IEC 27002, um processo formal de gerenciamento de senha do usuário deve

(A) solicitar ao usuário a assinatura de uma declaração de compromisso de manutenção da confidencialidade de sua senha pessoal e das senhas de grupos de trabalho.
(B) garantir que senhas temporárias sejam difíceis de ser adivinhadas e sejam iguais para todos os usuários eventuais.
(C) assegurar que senhas padrão possam ser usadas enquanto não for necessário aumentar o nível de segurança do sistema.
(D) implementar um procedimento para que senhas temporárias sejam enviadas, de modo seguro, para os endereços de e-mail fornecidos pelos usuários.
(E) instruir o usuário a não acusar o recebimento de senhas.

46

De acordo com a Norma NBR ISO/IEC 27002, o objetivo da classificação da informação é

(A) definir a que áreas de negócio a informação se destina.
(B) definir em que áreas de negócio as informações são produzidas.
(C) assegurar que a informação receba um nível adequado de proteção.
(D) assegurar que a informação seja confiável.
(E) assegurar que a informação adicione valor às atividades de uma organização.

47

Políticas de Segurança da Informação classificam os incidentes de segurança em níveis de severidade.

Qual incidente é classificado como de alto nível de severidade?

(A) Perda de senha
(B) Invasão de redes e sistemas
(C) Realização de download ilegal de músicas
(D) Utilização de recursos para fins pessoais
(E) Acesso a recurso não autorizado

48

Em muitos ambientes, as estações de clientes que usam a Internet estão posicionadas dentro de regiões protegidas por firewalls. Como se trata de estações de clientes, não é incomum que as regras do firewall impeçam a entrada de solicitações externas para o estabelecimento de conexões TCP (via SYN) com essas estações. Esse cenário gera um problema para o protocolo FTP, já que o servidor FTP é, normalmente, o encarregado de abrir uma conexão de dados com o cliente sempre que um comando STOR ou RETR é recebido através da conexão de controle.

Uma solução para esse problema é

(A) habilitar, no firewall, o recebimento de solicitações externas para estabelecer conexões TCP com portas 80, 81, 8080 e 8081 do cliente.
(B) habilitar no firewall, o recebimento de solicitações externas para estabelecer conexões TCP com a porta 21 do cliente.
(C) usar o FTP em modo ativo, pois isso fará com que o cliente passe a aceitar todas as conexões solicitadas em suas portas 20 e 21, eliminado o bloqueio do firewall nessas situações.
(D) usar o FTP em modo passivo, pois isso fará com que o servidor, em vez de solicitar a conexão pela porta de dados, fique à espera (listen) de uma solicitação de conexão vinda do cliente.
(E) usar um firewall com estado (stateful firewall), já que isso permitirá guardar o estado de conexões já estabelecidas (controle e dados) e, a partir daí, admitir as solicitações adequadas para conexão com a porta de dados do FTP do cliente.

49

O protocolo TFTP é uma alternativa simples para a transferência de arquivos, que foi projetado para ser fácil de implementar, porém com menos facilidades que outros protocolos, como, por exemplo, o FTP.

Uma das características do TFTP é que ele

(A) foi projetado para ser usado sobre um serviço de transporte orientado à conexão como o TCP.
(B) foi projetado para permitir que a transferência dos arquivos ocorra em blocos de qualquer tamanho desejado.
(C) permite apenas a transferência de arquivos texto codificados em ASCII.
(D) usa apenas dois tipos de pacotes: o Read request (RRQ) e o Write request (WRQ).
(E) não faz a autenticação dos usuários.

50

Considere uma subrede que use IPv4 com 200 estações e um único roteador de acesso para a Internet que implemente NAPT (Network Address Port Translation – algumas vezes também conhecido por PAT – Port Based Address Translation). A rede tem endereço interno local 10.0.0.0 e as 200 estações compartilham um mesmo endereço interno global 196.54.18.9. Considere ainda que a estação 10.0.0.204 envia uma requisição HTTP ao servidor 204.81.12.12:80. Essa requisição, ao atingir o servidor, fará com que ele gere uma resposta HTTP de volta à origem.

A requisição e a resposta HTTP, ao trafegarem pela Internet, serão endereçadas, respectivamente, a

(A) 196.54.18.9:80 e 10.0.0.204:7211
(B) 196.54.18.9.80 e 204.81.12.12:80
(C) 204.81.12.12:80 e 10.0.0.204:8080
(D) 204.81.12.12:80 e 196.54.18.9:7211
(E) 204.81.12.12:8080 e 196.54.18.9:80

51

Algumas distribuições recentes do sistema Linux, como o SUSE Enterprise Server, já utilizam um mecanismo de inicialização especificado em uma interface conhecida como UEFI (Unified Extensible Firmware Interface).

Uma das características desse mecanismo é que ele

(A) depende exclusivamente da interface de boot fornecida pela BIOS da estação, mantendo a compatibilidade com todos os sistemas anteriores.
(B) identifica o kernel autenticado para inicializar o sistema, reduzindo o potencial de ataques maliciosos nessa fase inicial de carga do sistema.
(C) não pode atuar em processadores da linha Intel nem em sistemas MS Windows.
(D) não permite o boot a partir de partições maiores do que 2TiB.
(E) não permite o boot a partir de partições menores do que 2 Gb.

52

O administrador de uma rede com estações Windows e Linux recebeu uma requisição para que fosse instalado algum recurso capaz de permitir que as estações Windows passassem a ter acesso aos arquivos e às impressoras dos servidores Linux.

Para essa tarefa, o administrador poderá instalar o software

(A) Samba nas estações Windows clientes
(B) Samba nas estações Linux servidoras
(C) Squid nas estações Windows clientes
(D) Squid nas estações Linux servidoras
(E) VNC nas estações Linux servidoras e nas Windows clientes

53

Na administração de um servidor Linux Red Hat, uma das formas mais fáceis de gerenciar as atualizações de pacotes de software no formato RPM é a utilização do software

(A) kerberos
(B) OpenSSL
(C) yum
(D) Xtables
(E) VNC

54

Syslog é um protocolo mantido pelo IETF cujo objetivo é

(A) acionar todas as proteções de um firewall para que o nível de segurança da rede seja levantado ao estágio mais protegido possível, ativando a gravação de toda a atividade da rede durante o período em que esse nível de proteção for mantido.
(B) enviar mensagens periódicas de aviso sobre a existência de um determinado serviço instalado em uma rede, o qual deve ser conhecido por estações clientes que desejem acesso a esse serviço.
(C) habilitar o recebimento, em modo promíscuo, de mensagens por um conjunto de estações especiais, chamadas gerentes, para que essas possam coletar informações da rede e detectar possíveis violações de segurança.
(D) impedir a autenticação de novos usuários durante um período determinado de tempo, durante o qual o sistema guardará todas as tentativas de autenticação para futura avaliação do administrador do sistema.
(E) permitir o envio de mensagens de notificação de eventos que permitam diagnosticar, resolver e administrar condições específicas de segurança, funcionamento e desempenho geral de dispositivos.

55

Considere as seguintes regras iptables:

```
iptables –flush
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

O resultado da aplicação dessas regras será a

(A) liberação do tráfego HTTP que chega a uma interface Eternet (eth0) de um servidor.
(B) liberação de todas as solicitações HTTP que são enviadas por um cliente para uma estação específica (eth0).
(C) não liberação do tráfego HTTP que chega a uma interface Eternet (eth0) de um servidor.
(D) não liberação de todas as solicitações HTTP que são enviadas por um cliente para outras estações.
(E) não liberação de todas as solicitações HTTPS que são enviadas por um cliente para outras estações.

56

Para testar o código de saída do último comando executado num script da bash (Bourne-Again Shell) e encerrar a execução desse script, caso o comando tenha sido executado sem erros, deve-se escrever a linha de código

(A) if [$? –eq 1]; then exit; fi
(B) if [$? –eq 0]; then exit; fi
(C) if [$# –eq 1]; then exit; fi
(D) if [$# –eq 0]; then exit; fi
(E) if [$? –eq 1 –a $# -eq 0]; then exit; fi

57

O trecho de código do script abaixo opera sobre o arquivo /etc/passwd.

```
AUX=`cat /etc/passwd | cut -d: -f3 | sort -n -r | tail -1`
echo $AUX
```

Esse trecho de código do script imprime o número do

(A) GID (Group Identification) usado pelo root.
(B) menor GID (Group Identification) usado no sistema.
(C) maior GID (Group Identification) usado no sistema.
(D) menor UID (User Identification) usado no sistema.
(E) maior UID (User Identification) usado no sistema.

58

Para configurar a tarefa /root/bin/tarefa a ser executada pelo cron, de meia em meia hora, toda segunda, quarta e sexta-feiras, deve-se configurar a linha de agendamento da tarefa com

(A) `00,30 * * * 1,3,5 /root/bin/tarefa`
(B) `00,30 * * * 2,4,6 /root/bin/tarefa`
(C) `30 * * * 1,3,5 /root/bin/tarefa`
(D) `30 * * * 2,4,6 /root/bin/tarefa`
(E) `30 * * * 2-4-6 /root/bin/tarefa`

59

A assinatura digital, presente no certificado digital emitido por uma Autoridade Certificadora (AC) para uma pessoa, visa a garantir a(o)

(A) integridade do certificado digital e a autenticidade da pessoa
(B) integridade e a autenticidade do certificado digital
(C) integridade, a autenticidade e o sigilo do certificado digital
(D) integridade e o sigilo do certificado digital
(E) sigilo do certificado digital, apenas

60

O efeito avalanche do algoritmo de resumo de mensagem está relacionado à sua propriedade de produzir digests

(A) iguais, para informações com alto grau de semelhança.
(B) diferentes, para informações com alto grau de semelhança.
(C) com criptografia reversível, para informações com alto grau de diferença entre si.
(D) com criptografia irreversível, para informações com alto grau de semelhança.
(E) não colidentes se as informações tiverem alto grau de diferença entre si.

61

O processo de autenticação forte é baseado em dois ou mais fatores.

Exemplos de fatores relacionados a algo que o usuário possui são

(A) senha pessoal e chave privada
(B) senha pessoal e cartão inteligente
(C) chave privada e cartão inteligente
(D) modelo biométrico e token
(E) modelo biométrico e lista TAN

62
Dentre as etapas necessárias para a validação de uma assinatura digital de documento assinado por um usuário, um sistema de validação de assinaturas deve decriptar a assinatura digital do usuário que assinou o documento com a(o) sua(seu)

(A) chave secreta
(B) chave privada
(C) chave pública
(D) chave simétrica
(E) certificado digital

63
Os algoritmos MD-5 e SHA-1 são exemplos de algoritmos que produzem resumo de mensagem (hash) e geram, em bits, respectivamente, digests com tamanho de

(A) 96 e 160
(B) 96 e 256
(C) 128 e 160
(D) 128 e 256
(E) 128 e 512

64
O ataque de negação de serviço (DoS) é uma tentativa de impedir que usuários legítimos de um serviço possam utilizá-lo.

Uma forma clássica desse tipo de ataque é a(o)

(A) inundação do alvo
(B) invasão de conta do usuário em redes sociais
(C) invasão do e-mail do usuário
(D) quebra de senhas dos usuários do alvo
(E) roubo de dados pessoais

65
Em um ataque DDoS, um grande número de hosts comprometidos é reunido para enviar pacotes inúteis.

No ataque de inundação SYN, o tipo de mensagem enviada pelos hosts escravos e o tipo endereço IP de origem, presente nos pacotes destinados ao alvo, respectivamente, são:

(A) RST do TCP; legítimo
(B) ACK do TCP; falso
(C) SYN/ACK do TCP; legítimo
(D) SYN/ACK do TCP; falso
(E) SYN do TCP; falso

66
Um projeto de cabeamento estruturado requer uma frequência de transmissão de até 500 MHz, em 100 metros, para atender os requisitos de redes 10Gbps.

Nesse projeto, pode ser utilizado cabo de par trançado da(s) categoria(s)

(A) 5e, apenas
(B) 6, apenas
(C) 6a, apenas
(D) 5e e 6
(E) 6 e 6a

67
Para elevar o nível de segurança da comunicação entre aplicações, o IETF (Engineering Task Force) definiu o TLS Protocol v1.0 para fornecer privacidade e integridade dos dados.

Esse protocolo é composto pelas camadas

(A) TLS Record Protocol e TLS Handshake Protocol, apenas
(B) TLS Encapsulating Protocol e TLS Integrity Protocol, apenas
(C) TLS Encapsulating Protocol e TLS Record Protocol, apenas
(D) TLS Encapsulating Protocol, TLS Integrity Protocol e TLS Handshake Protocol
(E) TLS Integrity Protocol, TLS Record Protocol e TLS Handshake Protocol

68
A configuração de teste para certificação do cabeamento instalado, reconhecido para as categorias 5e, 6 e 6a, no modelo de canal, considera

(A) o cabo horizontal e o cabo de transição (se houver), apenas
(B) o cabo horizontal, o cabo de transição (se houver) e o cordão do equipamento ativo, apenas
(C) o cabo horizontal, o cabo de transição (se houver) e o cordão de manobra (patch cord de cross connect), apenas
(D) o cabo horizontal, o cabo de transição (se houver), o cordão do equipamento ativo e o cordão de manobra (patch cord de cross connect), apenas
(E) todos os cabos e cordões, ou seja, o cabo horizontal, o cabo de transição (se houver), o cordão do equipamento ativo, o cordão de manobra (patch cord de cross connect) e o cordão do usuário na área de trabalho.

69
O processo de transmissão da luz ao longo da fibra óptica é feito através da reflexão interna total. Quando o diâmetro da fibra é reduzido a alguns comprimentos de onda da luz, a fibra age como um guia de onda.

O modo como a luz se propaga e o(s) tipo(s) de fibra(s) caracterizada(s), respectivamente, são:

(A) em linha reta, sem ricochetear em diferentes ângulos; monomodo
(B) em linha reta, sem ricochetear em diferentes ângulos; multimodo
(C) em linha reta, sem ricochetear em diferentes ângulos; monomodo e multimodo
(D) dispersa, ricocheteando em diferentes ângulos; monomodo
(E) dispersa, ricocheteando em diferentes ângulos; multimodo

70

Um administrador de rede deseja monitorar o tráfego de rede para identificar a ocorrência de atividades maliciosas e violações da política de segurança da empresa.

O componente do perímetro de segurança capaz de executar essa tarefa com base na anomalia e na assinatura do tráfego de rede é o

(A) gateway VPN
(B) firewall de estado
(C) firewall proxy
(D) filtro de pacotes
(E) sistema de detecção de intrusão

RASCUNHO

RASCUNHO