이름: _____ 날짜: _____ 점수: _____

원격 접속 VPN

원격 인력의 엔드포인트 보호, 다중 인증, IPsec 터널 구성.

원격 접속 VPN 학습 개요

학습자
학생 신분
네트워크 수비 트랙

보안
연결 상태
데이터 패킷 보호하기

켜짐
유출 방지
DNS 및 IPv6 유출 방지

환영합니다! 이 활동 자료집은 원격 접속 VPN 네트워크를 안내합니다. 클라이언트-사이트 터널, 다중 인증 로그인, 엔드포인트 상태 점검, 대역폭 제한, syslog 보안 감사를 살펴봅니다.

워크시트 체크포인트

- [ ] **파트 1-4: VPN과 네트워크 보안 구성을 익힙니다.**
- [ ] **파트 5-7: 십자말풀이와 단어 찾기 퍼즐을 풉니다.**
- [ ] **파트 8-9: 사례 연구와 암호 도전 과제를 풉니다.**
- [ ] **파트 10: 기초 및 심화 FAQ 페이지를 살펴봅니다.**
- [ ] **파트 11: 흥미로운 실제 사실 10가지를 살펴봅니다.**
- [ ] **보너스: 빠르게 생각하기 도전**

VPN.com 최고의 VPN 가이드 열기

URL: https://www.vpn.com/vpn/best-vpn-for-business/remote-access/

나의 원격 접속 VPN 학습 로드맵

- 로컬 네트워크 노드에 접근하는 원격 인력의 엔드포인트를 보호하기.
- 원격 로그인에 대한 다단계 인증 정책을 구성하세요.
- 클라이언트-사이트 IPsec 및 OpenVPN 구성 설정하기.
- 접근 통제 위반이 있는지 원격 연결 로그를 점검하세요.
- 네트워크 연결을 허용하기 전에 기기 상태 점검을 도입하세요.
- 재택근무 대역폭 병목을 막도록 서버 처리량을 최적화하세요.

원격 접속 VPN 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 보안 상태 점검과 다중 인증 로그인에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

클라이언트 대 사이트 터널과 엔드포인트 규정 준수(소개)

원격 접속 VPN은 외부에서 근무하는 직원을 위한 안전한 클라이언트-사이트 터널을 만듭니다. 이런 연결을 보호하려면 다중 인증(MFA) 로그인을 적용하고, 엔드포인트 상태 규정 준수 검사를 수행하며, 중앙 syslog 수집기로 로그를 감사해야 합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 원격 접속 VPN 포털에서 의무화해야 하는 인증 표준은 무엇입니까?

- A) 다중 인증
- B) 단일 요소
- C) 암호화되지 않음
- D) 로컬 게스트

2. 원격 근무의 클라이언트-사이트 간 연결을 보호하는 표준 프로토콜은 무엇입니까?

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3. 연결하기 전에 원격 노트북이 깨끗한지 확인하는 검사는 무엇입니까?

- A) 상태 점검
- B) 속도 테스트
- C) 핑 테스트
- D) 메모리 수

4. 보안 감사를 위해 원격 근무자의 연결 로그는 어디에 저장됩니까?

- A) Syslog 서버
- B) 레지스트리 키
- C) 클라이언트 메모리
- D) 웹 브라우저

5. 원격 근무자 수가 게이트웨이 대역폭 용량을 넘으면 어떤 문제가 발생합니까?

- A) 대역폭 제한
- B) DNS 누출
- C) 핸드셰이크 통과
- D) IP 노출

체크포인트 2: 참/거짓 도전

6 질문 6

6. 다중 요소 인증은 원격 로그인을 보호하기 위해 보조 검증 토큰을 추가합니다.

○ 참 ○ 거짓

7 질문 7

7. 보안 상태 점검은 방화벽이 꺼진 원격 기기가 비공개 서버에 접근하도록 허용합니다.

○ 참 ○ 거짓

8 질문 8

8. 원격 접속 VPN 로그는 회사 네트워크에 대한 무단 접근을 추적하는 데 필수입니다.

○ 참 ○ 거짓

9 질문 9

9. OpenVPN과 IPsec은 원격 클라이언트 페이로드를 암호화하지 못하는 구식 프로토콜입니다.

○ 참 ○ 거짓

10 질문 10

10. 게이트웨이 대역폭 병목은 원격 트래픽이 연결 카드의 용량을 초과할 때 발생합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

아래 각 문장을 읽고 단어 목록에서 알맞은 용어를 골라 빈칸을 채우세요.

1. 회사 포털을 보호하려면 원격 로그인에 _____ 인증이 필요합니다.
2. 원격 클라이언트는 표준 _____ 프로토콜로 터널 페이로드 데이터를 암호화합니다.
3. 기기는 네트워크에 연결되기 전에 보안 _____ 점검을 통과해야 합니다.
4. 감사 가능한 접속 로그는 중앙 _____ 서버로 지속적으로 전송됩니다.
5. 업무 시간대의 대량 트래픽은 게이트웨이 _____ 혼잡을 일으킬 수 있습니다.
6. 가상 어댑터 드라이버는 윈도우와 맥OS에서 클라이언트-사이트 간 _____ 을(를) 처리합니다.

어휘 단어 목록

다중 | 대역폭 | 방화벽 | 상태 | 시스로그 | 오픈VPN | 원격 근무 | 터널링

여기에 답을 쓰세요:

1.
2.
3.
4.
5.
6.

체크포인트 4: 핵심 개념 연결

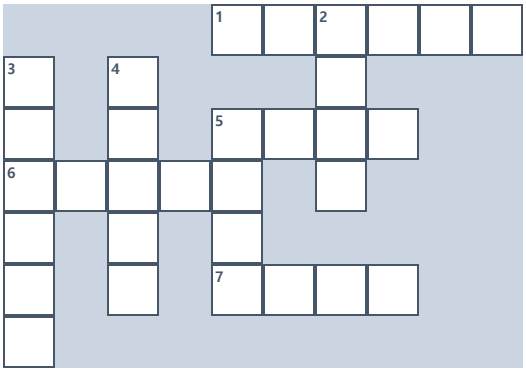
정의 연결하기

왼쪽의 각 어휘를 오른쪽의 알맞은 설명과 연결하고, 입력 칸에 해당하는 글자(A-H)를 쓰세요.

☐	**1. 다중 요소**	**A**	데이터를 보안 경로에 캡슐화하는 것.
☐	**2. OpenVPN**	**B**	중앙 보안 로그 수집기.
☐	**3. 보안 상태**	**C**	네트워크 데이터 용량 한계.
☐	**4. SYSLOG**	**D**	표준 클라이언트-사이트 프로토콜.
☐	**5. 대역폭**	**E**	원격 기기 상태 검증.
☐	**6. 암호화**	**F**	트래픽 필터링 시스템 규칙입니다.
☐	**7. 터널링**	**G**	패킷을 암호화로 뒤섞는 것.
☐	**8. 방화벽**	**H**	추가 토큰을 요구하는 로그인 보안.

체크포인트 5: 십자말풀이

활성화된 흰색 칸에 글자를 입력해 십자말풀이를 푸세요. 숫자는 아래 열쇠에 해당합니다.



가로

1. 원격 기기의 상태를 검증하는 일 (6)
5. 접속하는 장치의 보안 상태를 살펴보는 일 (4)
6. 데이터를 보안 경로 안에 캡슐화하는 일 (5)
7. 사무실 밖에서 네트워크에 접속해 일하는 방식 (4)

세로

2. 기기가 안전한 상태인지 살펴보는 일 (4)
3. 패킷을 암호로 뒤섞는 일 (6)
4. 암호화된 통로를 만드는 방식에 대한 규칙 (5)
5. 문제가 생기면 도와주는 서비스 (4)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

화면 낭독기와 키보드 사용자는 아래 입력란에 십자말풀이 정답을 직접 입력할 수 있습니다.

가로

1 가로: 원격 기기의 상태를 검증하는 일 (6 글자):

5 가로: 접속하는 장치의 보안 상태를 살펴보는 일 (4 글자):

6 가로: 데이터를 보안 경로 안에 캡슐화하는 일 (5 글자):

7 가로: 사무실 밖에서 네트워크에 접속해 일하는 방식 (4 글자):

세로

2 세로: 기기가 안전한 상태인지 살펴보는 일 (4 글자):

3 세로: 패킷을 암호로 뒤섞는 일 (6 글자):

4 세로: 암호화된 통로를 만드는 방식에 대한 규칙 (5 글자):

5 세로: 문제가 생기면 도와주는 서비스 (4 글자):

체크포인트 6: 숨은 단어 찾기

아래 격자에 숨어 있는 핵심 어휘 8개를 찾으세요. 단어는 가로, 세로, 대각선으로 배치될 수 있습니다.

라	인	요	다	서	링	하	크	규	주	증	도	타	밀	개
접	화	트	격	밀	라	소	술	기	카	다	스	방	속	크
무	검	타	파	라	전	크	기	기	술	메	전	안	연	안
격	점	넷	타	바	스	근	링	다	트	지	터	응	용	기
근	기	결	템	색	기	다	널	험	넷	파	원	넷	칙	데
지	기	격	상	버	기	공	터	밀	자	시	술	네	송	리
번	격	점	위	결	상	아	요	널	템	메	하	암	인	바
가	마	아	속	상	태	암	넷	태	링	벽	점	소	방	타
검	관	데	터	타	검	술	전	이	화	규	위	공	워	이
점	이	험	리	템	증	요	주	트	사	도	칙	위	결	호
태	데	이	터	암	호	화	스	바	널	카	도	원	답	원
상	아	근	널	버	화	크	무	카	전	타	관	칙	격	공
사	청	마	가	무	연	카	벽	나	타	결	타	근	안	크
술	카	리	험	데	하	술	스	근	도	안	무	관	검	보
나	다	관	속	전	공	소	상	위	넷	시	요	스	차	전

어휘 단어 목록

터널링규칙 · 기기점검 · 기기상태검증 · 상태점검 · 기술지원 · 데이터암호화 · 터널링기술 · 원격근무

체크포인트 6 대체 활동: 접근성을 고려한 어휘 연결

단어 찾기의 8개 어휘를 각각 알맞은 설명과 연결하고, 빈칸에 글자(A-H)를 쓰세요.

어휘 용어

- **A. 터널링규칙**
- **B. 기기점검**
- **C. 기기상태검증**
- **D. 상태점검**
- **E. 기술지원**
- **F. 데이터암호화**
- **G. 터널링기술**
- **H. 원격근무**

정의 및 연결 항목

1. 기기가 안전한 상태인지 살펴보는 일.
2. 사무실 밖에서 네트워크에 접속해 일하는 방식.
3. 데이터를 보안 경로 안에 캡슐화하는 일.
4. 패킷을 암호로 뒤섞는 일.
5. 접속하는 장치의 보안 상태를 살펴보는 일.
6. 문제가 생기면 도와주는 서비스.
7. 원격 기기의 상태를 검증하는 일.
8. 암호화된 통로를 만드는 방식에 대한 규칙.

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 이 워크시트의 핵심 개념을 알아내세요. 정답을 제공된 입력란에 쓰세요.

1. 규 링 터 칙 널 _____
2. 증 기 상 검 태 기 _____
3. 원 기 지 술 _____
4. 링 술 기 터 널 _____
5. 검 기 점 기 _____
6. 점 검 상 태 _____
7. 호 데 암 화 터 이 _____
8. 원 무 근 격 _____

보너스 활동: 빠르게 생각하기

각 범주마다 답을 3개씩 쓰세요. 목록을 가장 먼저 채운 사람이 이깁니다.

1	VPN에 대한 오해			
2	제로 트러스트를 설명하는 단어			
3	알고 있는 사무용 프로그램			
4	안전한 원격 근무를 위한 규칙			
5	인터넷 서비스 제공업체가 볼 수 있는 것			
6	알고 있는 VPN 서비스			
7	직원들이 일하는 장소			
8	회사가 매일 사용하는 도구			
9	IT 부서의 역할			
10	직원이 가지고 있을 수 있는 기기			
11	회사가 보호해야 하는 데이터			
12	보안 침해 후에 할 일			
13	화상 회의를 방해할 수 있는 것			
14	안전하게 로그인하는 방법			
15	직원에게 VPN을 제공하는 이유			

체크포인트 8: VPN 및 네트워크 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: MFA 의무화



상황: 한 비즈니스 분석가가 원격 근무 중에 회사 데이터베이스에 로그인하려고 합니다. 사용자 이름과 비밀번호는 올바르게 입력했지만, VPN 포털이 접속을 차단하고 물리적 토큰 코드를 요구합니다.

토론 질문: 어떤 보안 정책이 이 이중 확인 단계를 강제하고 있습니까?

사례 연구 2: 보안 상태 규정 준수



상황: 한 계약직 직원이 개인 노트북을 원격 회사 네트워크에 연결합니다. VPN 클라이언트가 즉시 연결을 끊고, 백신 정의 파일이 오래되었다고 사용자에게 알립니다.

토론 질문: 이 연결 시도를 차단한 특수한 VPN 게이트웨이 검사는 무엇입니까?

체크포인트 9: 암호 해독하기

네트워크 엔지니어는 라우팅 채널과 클라이언트 터널을 보호합니다. 아래의 자모-숫자 키를 사용해 해당하는 자모를 빈칸에 써서 메시지를 해독하세요.

자모-숫자 암호화 키

ㄱ=1 ㄲ=2 ㄴ=3 ㄷ=4 ㄸ=5 ㄹ=6 ㅁ=7 ㅂ=8 ㅃ=9 ㅅ=10
ㅆ=11 ㅇ=12 ㅈ=13 ㅉ=14 ㅊ=15 ㅋ=16 ㅌ=17 ㅍ=18 ㅎ=19 ㅏ=20
ㅐ=21 ㅑ=22 ㅒ=23 ㅓ=24 ㅔ=25 ㅕ=26 ㅖ=27 ㅗ=28 ㅘ=29 ㅙ=30
ㅚ=31 ㅛ=32 ㅜ=33 ㅝ=34 ㅞ=35 ㅟ=36 ㅠ=37 ㅡ=38 ㅢ=39 ㅣ=40

12	34	3	1	26	1		13	24	8	10	28	1	12	38	6	28

8	33	3	10	20	3		1	40	1	40		8	28	19	28

해독된 메시지:

팁: 각 숫자는 아래 키의 한글 자모 하나를 나타냅니다. 자모를 차례로 모아 글자를 만드세요(예: ㅂ+ㅗ = 보).

체크포인트 10: 기초 VPN FAQ (파트 A)

가상 사설망(VPN)과 터널링에 관해 가장 자주 묻는 질문과 답을 살펴보세요.

Q1: 원격 접속 VPN이란 무엇인가요?

외부에서 근무하는 직원이 비공개 기업 서버에 직접 연결할 수 있게 하는 보안 연결 방식.

Q2: 클라이언트-사이트 방식이 사이트-사이트 방식과 다른 이유는 무엇인가요?

클라이언트 대 사이트는 개별 사용자 기기를 연결하고, 사이트 대 사이트는 물리적 사무실 전체를 연결합니다.

Q3: 기기 상태 점검이란 무엇인가요?

접근을 허용하기 전에 원격 기기의 보안 상태(백신, OS 패치 수준)를 점검하는 검사.

Q4: 원격 접속에 OpenVPN을 사용하는 이유는 무엇인가요?

강력한 보안 프로토콜, 크로스 플랫폼 호환성, 개별 연결을 처리하는 능력 때문입니다.

Q5: MFA는 원격 접속을 어떻게 보호하나요?

추가 인증 토큰을 더해, 직원 비밀번호가 유출되거나 도난당해도 접근을 막습니다.

체크포인트 10: 기초 VPN FAQ (파트 B)

가상 사설망(VPN)과 터널링에 관해 가장 자주 묻는 질문과 답을 살펴보세요.

Q6: syslog 서버란 무엇인가요?

규정 준수 감사를 위해 연결 이벤트, 로그인, 시스템 경고를 저장하는 중앙 집중형 로그 저장소.

Q7: 대역폭 병목의 원인은 무엇인가요?

원격 직원들의 총 대역폭 수요가 회사 게이트웨이의 인터넷 속도 상한을 넘을 때.

Q8: 집 컴퓨터를 회사 VPN에 연결할 수 있나요?

기기가 기업의 보안 상태 점검 감사를 통과하고 IT 관리자가 승인한 경우에만 가능합니다.

Q9: 네트워크 캡슐화란 무엇인가요?

전송을 안전하게 하기 위해 이동 중인 데이터 패킷을 암호화된 프로토콜 헤더로 감싸는 것입니다.

Q10: 스플릿 터널링은 원격 접속을 어떻게 최적화하나요?

직원이 일반 탐색에는 로컬 ISP를 사용하고 업무 관련 파일만 VPN을 통해 라우팅할 수 있게 합니다.

체크포인트 10: 심화 VPN FAQ (파트 C)

VPN 터널링 프로토콜, 모바일 클라이언트 통합, 기업 배포의 고급 기술적 측면을 탐구합니다.

Q1: 인증서 기반 인증은 원격 접속을 어떻게 강화하나요?

연결 권한을 미리 설치된 로컬 디지털 인증서에 연동하여 관리되지 않거나 승인되지 않은 기기를 차단합니다.

Q2: 재택근무에서 스플릿 터널링의 보안 위험은 무엇인가요?

침해된 로컬 기기가 외부 위협을 사설 네트워크로 전달하는 다리가 될 수 있습니다.

Q3: 상태 점검은 레지스트리 설정을 어떻게 검사하나요?

VPN 클라이언트는 로컬 스크립트를 실행하여 레지스트리 경로를 조회하고 기업 보안 소프트웨어가 실제로 실행 중인지 확인합니다.

Q4: syslog가 기본적으로 UDP 포트 514를 사용하는 이유는 무엇인가요?

최소한의 오버헤드로 로그를 빠르게 전송하기 위해서이지만, 안전한 구성에서는 이제 TCP 위의 TLS 캡슐화를 의무로 합니다.

Q5: 기업은 게이트웨이 대역폭 병목을 어떻게 해결하나요?

로드 밸런서를 구현하고 원격 트래픽을 지역별 서버 노드에 분산함으로써.

체크포인트 10: 심화 VPN FAQ (파트 D)

VPN 터널링 프로토콜, 모바일 클라이언트 통합, 기업 배포의 고급 기술적 측면을 탐구합니다.

Q6: 원격 클라이언트에서 가상 TAP/TUN 어댑터의 기능은 무엇인가요?

가상 네트워크 카드처럼 작동하여 기기 수준의 TCP/IP 트래픽을 암호화된 VPN 터널로 바로 보냅니다.

Q7: IKEv2 MOBIKE는 원격 근무 인력의 이동성을 어떻게 지원하나요?

IP 주소 바인딩을 동적으로 업데이트하여 사용자가 Wi-Fi와 이동통신 데이터 사이를 오가도 VPN이 활성 상태로 유지됩니다.

Q8: 분할 라우팅과 전체 터널 라우팅은 어떻게 다른가요?

전체 라우팅은 기기의 모든 인터넷 트래픽을 VPN으로 보내지만, 분할 라우팅은 회사 대상 IP만 보냅니다.

Q9: NAT 장치는 원격 VPN 연결을 어떻게 처리하나요?

로컬 포트 범위를 공인 게이트웨이 IP 주소에 매핑하여 돌아오는 암호화 데이터 패킷을 라우팅함으로써.

Q10: 어떤 규정 준수 표준이 원격 접속 감사를 의무화하나요?

HIPAA, SOC 2, PCI DSS 같은 표준은 모든 원격 연결 세션을 기록하고 모니터링할 것을 요구합니다.

파트 11: 실제 VPN 사실 10가지와 시사점

VPN 암호화 속도, 프로토콜 감사, 모바일 연결, 기업의 원격 근무에 관한 실제 사실을 살펴보세요.

1. VPN 인사이트

원격 접속 VPN은 외부에서 근무하는 직원을 위한 안전한 클라이언트-사이트 터널을 만듭니다.

2. VPN 인사이트

규정 준수 규칙에 따라 원격 업무 포털을 보호하려면 다중 요소 인증이 필요합니다.

3. VPN 인사이트

보안 상태 점검은 비공개 네트워크 접근을 허용하기 전에 로컬 클라이언트의 보안 설정을 확인합니다.

4. VPN 인사이트

Syslog 서버는 연결 로그를 모아 무단 접근 시도를 감사하고 탐지합니다.

5. VPN 인사이트

게이트웨이 대역폭 병목은 원격 트래픽 총수요가 서버의 인터넷 한도를 초과할 때 발생합니다.

6. VPN 인사이트

가상 네트워크 어댑터는 운영체제의 네트워크 쿼리를 보안 프로토콜 안에 캡슐화합니다.

7. VPN 인사이트

MOBIKE를 지원하면 원격 클라이언트가 VPN 터널이 끊기지 않은 채로 네트워크를 전환할 수 있습니다.

8. VPN 인사이트

전체 터널 라우팅은 직원의 모든 인터넷 트래픽을 보호하지만 회사 게이트웨이의 부하를 높입니다.

9. VPN 인사이트

인증서 인증은 VPN 연결 승인을 회사에서 관리하는 하드웨어에 직접 연결합니다.

10. VPN 인사이트

SOC 2, PCI DSS 같은 프레임워크는 원격 접속 세션의 로깅과 모니터링을 요구합니다.

기술 참고 자료 및 출처

이 학습 가이드와 인터랙티브 퍼즐은 전 세계 기술 표준, 사양, 규제 체계를 바탕으로 만들었습니다.

학술 및 업계 참고 자료

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

답안: 체크포인트 1 – 객관식

1 로그인 토큰 MFA 보안 정답: A

교사용 참고

다중 요소 인증은 로그인 시 보조 검증을 요구합니다. 출처: MFA Implementation.

2 OpenVPN 터널 클라이언트 대 사이트 정답: A

교사용 참고

OpenVPN은 클라이언트-사이트 간 터널을 보호하는 표준 프로토콜입니다. 인용: OpenVPN Client.

3 보안 상태 감사 기기 확인 정답: A

교사용 참고

보안 상태 점검은 엔드포인트에서 방화벽과 백신 도구가 활성화되어 있는지 검사합니다. 인용: Posture Compliance.

4 로그 수집기 SYSLOG 서버 정답: A

교사용 참고

Syslog 서버는 보안 이벤트 로그를 수집해 접근 위반을 모니터링합니다. 출처: Syslog 표준.

5 카드 한도 초과 게이트웨이 병목 정답: A

교사용 참고

게이트웨이 대역폭 병목은 사용자 트래픽이 서버 한도를 초과할 때 발생합니다. 출처: Capacity Planning.

답안: 체크포인트 2 – 참 또는 거짓

6 **로그인 토큰** MFA 확인 정답: 참

교사용 참고

다중 요소 인증은 로그인 시 보조 검증을 요구합니다. 출처: MFA Implementation.

7 **질문 7** 정답: 거짓

교사용 참고

상태 점검은 방화벽이나 백신이 꺼져 있는 기기를 차단하므로 그런 기기는 접근이 거부됩니다.

8 **로그 수집기** SYSLOG 서버 정답: 참

교사용 참고

Syslog 서버는 보안 이벤트 로그를 수집해 접근 위반을 모니터링합니다. 출처: Syslog 표준.

9 **질문 9** 정답: 거짓

교사용 참고

OpenVPN과 IPsec은 원격 클라이언트 트래픽을 암호화하는 현재 사용 중인 프로토콜입니다.

10 **카드 한도 초과** 게이트웨이 병목 정답: 참

교사용 참고

게이트웨이 대역폭 병목은 사용자 트래픽이 서버 한도를 초과할 때 발생합니다. 출처: Capacity Planning.

어휘 정답 및 채점 기준표

교사용 채점 기준: 정확하게 연결한 항목마다 1점(총 8점), 문맥 용어마다 1점(총 6점)을 줍니다.

체크포인트 4: 답안 – 개념 연결

H 1. 다중 요소	D 2. OpenVPN	E 3. 보안 상태	B 4. SYSLOG
C 5. 대역폭	G 6. 암호화	A 7. 터널링	F 8. 방화벽

체크포인트 3: 답안 – 핵심 용어

1 다중	2 오픈VPN	3 상태	4 시스로그
5 대역폭	6 터널링		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 D – 상태점검	2 H – 원격근무	3 G – 터널링기술	4 F – 데이터암호화
5 B – 기기점검	6 E – 기술지원	7 C – 기기상태검증	8 A – 터널링규칙

교사를 위한 토론 참고

핵심 용어:
학생들이 다중 요소, OpenVPN, 보안 상태를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

사례 연구:
학생들이 의견이 아니라 워크시트의 사실을 근거로 권고안을 제시하게 하세요.

출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

라	인	요	다	서	링	하	크	규	주	증	도	타	밀	개
접	화	트	격	밀	라	소	술	기	카	다	스	방	속	크
무	검	타	파	라	전	크	기	기	술	메	전	안	연	안
격	점	넷	타	바	스	근	링	다	트	지	터	응	용	기
근	기	결	템	색	기	다	널	험	넷	파	원	넷	칙	데
지	기	격	상	버	기	공	터	밀	자	시	술	네	송	리
번	격	점	위	결	상	아	요	널	템	메	하	암	인	바
가	마	아	속	상	태	암	넷	태	링	벽	점	소	방	타
검	관	데	터	타	검	술	전	이	화	규	위	공	워	이
점	이	험	리	템	증	요	주	트	사	도	칙	위	결	호
태	데	이	터	암	호	화	스	바	널	카	도	원	답	원
상	아	근	널	버	화	크	무	카	전	타	관	칙	격	공
사	청	마	가	무	연	카	벽	나	타	결	타	근	안	크
술	카	리	험	데	하	술	스	근	도	안	무	관	검	보
나	다	관	속	전	공	소	상	위	넷	시	요	스	차	전

십자말풀이 정답

						기	기	상	태	검	증			
데		터						태						
이		널				기	기	점	검					
터	널	링	기	술				검						
암		규		지										
호		칙		원	격	근	무							
화														

십자말풀이 정답 교사용 안내

가로

1 가로: 기기상태검증 원격 기기의 상태를 검증하는 일 (6 글자)

5 가로: 기기점검 접속하는 장치의 보안 상태를 살펴보는 일 (4 글자)

6 가로: 터널링기술 데이터를 보안 경로 안에 캡슐화하는 일 (5 글자)

7 가로: 원격근무 사무실 밖에서 네트워크에 접속해 일하는 방식 (4 글자)

세로

2 세로: 상태점검 기기가 안전한 상태인지 살펴보는 일 (4 글자)

3 세로: 데이터암호화 패킷을 암호로 뒤섞는 일 (6 글자)

4 세로: 터널링규칙 암호화된 통로를 만드는 방식에 대한 규칙 (5 글자)

5 세로: 기술지원 문제가 생기면 도와주는 서비스 (4 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 규링터칙널 — **터널링규칙**
2. 증기상검태기 — **기기상태검증**
3. 원기지술 — **기술지원**
4. 링술기터널 — **터널링기술**
5. 검기점기 — **기기점검**
6. 점검상태 — **상태점검**
7. 호데암화터이 — **데이터암호화**
8. 원무근격 — **원격근무**

비밀 암호 도전 정답

"원격 접속으로 분산 기기 보호"

사례 연구 답안

A 사례 연구 1: MFA 의무화 교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 비즈니스 분석가가 원격 근무 중에 회사 데이터베이스에 로그인하려 합니다. 올바른 사용자 이름과 비밀번호를 입력했지만 VPN 포털이 접근을 막고 물리 토큰 코드를 요구합니다.
- 권장 전략 및 해결책: 회사 VPN 포털은 원격 로그인을 보호하기 위해 엄격한 다중 인증(MFA) 정책을 적용합니다.

B 사례 연구 2: 보안 상태 규정 준수 교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 계약직 직원이 개인 노트북을 원격 회사 네트워크에 연결합니다. VPN 클라이언트가 즉시 연결을 끊고, 백신 정의 파일이 오래되었다고 사용자에게 알립니다.
- 권장 전략 및 해결책: 원격 접속 게이트웨이가 엔드포인트 상태 점검을 수행했고, 보안 설정이 오래되어 해당 기기를 차단했습니다.