Co zapewnia zarówno bezpieczną segmentację, jak i ochronę przed zagrożeniami w rozwiązaniu Secure Data Center?

•Oprogramowanie Cisco Security Manager
•Serwer AAA
•Adaptacyjne urządzenie zabezpieczające
•system zapobiegania włamaniom

Jakie są trzy podstawowe komponenty rozwiązania Cisco Secure Data Center? (Wybierz trzy.) •sieć siatki
•bezpieczna segmentacja
•widoczność
•obrona przed zagrożeniem
•serwery
•infrastruktura

Jakie są trzy cechy trybu przezroczystego ASA? (Wybierz trzy.)

•Ten tryb nie obsługuje przekaźników VPN, QoS ani DHCP.
•Jest to tradycyjny tryb wdrażania zapory.
•Ten tryb jest określany jako "uderzenie w drut. "
•NAT można zaimplementować między połączonymi sieciami.
•W tym trybie ASA jest niewidoczny dla atakującego.
•Interfejsy oddzielnych sieci ASA warstwy 3 i wymagają adresów IP w różnych podsieciach.

Co jest potrzebne, aby określony ruch pochodzący z zewnętrznej sieci zapory ASA mógł dotrzeć do sieci wewnętrznej?

•ACL
•NAT
•dynamiczne protokoły routingu
•poza strefą bezpieczeństwa poziom 0

Które dwa zadania są związane z hartowaniem routera? (Wybierz dwa.)

•umieszczenie routera w bezpiecznym pomieszczeniu
•wyłączanie nieużywanych portów i interfejsów
•instalacja maksymalnej możliwej pamięci
•zapewnienie dostępu administracyjnego
•z wykorzystaniem zasilaczy bezprzerwowych

Jakie możliwości ochrony przed zagrożeniami zapewnia Cisco ESA?
•filtrowanie sieci
•bezpieczeństwo dostępu do chmury
•ochrona przed spamem
•Monitorowanie ruchu warstwy 4

Jakie są dwa środki bezpieczeństwa stosowane w celu ochrony punktów końcowych w sieci bez granic? (Wybierz dwa.)

•denylisting

•Przerwij IPS
•DLP
•DMZ
•rootkit

Jakie trzy typy ruchu są dozwolone, gdy wydano polecenie auto kontroli portu uwierzytelnienia, a klient nie został jeszcze uwierzytelniony? (Wybierz trzy.)

•CDP
•802,1Q
•IPsec
•TACACS +
•STP
•EAPOL

Które stwierdzenie opisuje cechę protokołu IKE?

•Wykorzystuje port UDP 500 do wymiany informacji IKE między bramami bezpieczeństwa.
•IKE Phase 1 można wdrożyć w trzech różnych trybach: głównym, agresywnym lub szybkim.
•Umożliwia transmisję kluczy bezpośrednio przez sieć.
•Celem IKE Phase 2 jest wynegocjowanie powiązania bezpieczeństwa między dwoma rówieśnikami IKE.

Jakie działania podejmują rówieśnicy IPsec podczas wymiany IKE Phase 2?
•wymiana kluczy DH
•negocjacje polityki IPsec
•negocjacje zestawów zasad IKE
•weryfikacja tożsamości rówieśniczej

Jakie dwa algorytmy skrótu są używane z IPsec AH w celu zagwarantowania autentyczności? (Wybierz dwa.)

•SHA
•RSA
•DH
•MD5
•AES

Co jest charakterystyczne dla opartego na rolach widoku CLI konfiguracji routera?
•Widok CLI ma hierarchię poleceń z coraz wyższymi widokami.
•Po usunięciu podglądu powiązane widoki CLI są usuwane.
•Pojedynczy widok CLI może być współdzielony w ramach wielu podglądów.
•Tylko użytkownik podglądu może skonfigurować nowy widok i dodać lub usunąć polecenia z istniejących widoków.

Jakie jest ograniczenie korzystania z zarządzania OOB w dużej sieci przedsiębiorstw?

•Ruch produkcyjny dzieli sieć z ruchem zarządzającym.
•Serwery terminali mogą mieć bezpośrednie połączenia konsoli z urządzeniami użytkownika wymagającymi zarządzania.
•Zarządzanie OOB wymaga utworzenia VPN.
•Wszystkie urządzenia wydają się być podłączone do jednej sieci zarządzania.

Które dwa typy hakerów są zazwyczaj klasyfikowane jako hakerzy w szarym kapeluszu? (Wybierz dwa.)

•haktywiści
•cyberprzestępcy
•brokerzy podatności
•dzieciaki ze skryptów
•hakerzy sponsorowani przez państwo

Opisując złośliwe oprogramowanie, jaka jest różnica między wirusem a robakiem?

•Wirus koncentruje się na uzyskaniu uprzywilejowanego dostępu do urządzenia, podczas gdy robak tego nie robi.

•Wirus replikuje się, dołączając do innego pliku, podczas gdy robak może replikować się niezależnie.

•Wirus może być użyty do przeprowadzenia ataku DoS (ale nie DDoS), ale robak może być użyty do uruchomienia zarówno ataków DoS, jak i DDoS.
•Wirus może być wykorzystywany do wyświetlania reklam bez zgody użytkownika, podczas gdy robak nie.

Którego typu pakietu nie można przefiltrować przez wychodzącą ACL?

•pakiet multiemisji
•Pakiet ICMP
•pakiet telewizyjny
•pakiet generowany przez router

Jaka technologia ma funkcję korzystania z zaufanych protokołów stron trzecich w celu wydawania poświadczeń, które są akceptowane jako autorytatywna tożsamość?

•podpisy cyfrowe
•algorytmy skrótu
•Certyfikaty PKI
•klucze symetryczne
Jakie są dwie metody utrzymania statusu odwołania certyfikatu? (Wybierz dwa.) •podległy CA

•OCSP
•DNS
•LDAP
•CRL

Który protokół jest standardem IETF, który definiuje format certyfikatu cyfrowego PKI?

•SSL / TLS
•X.500
•LDAP
•X.509

Jaki jest najlepszy sposób, aby zapobiec atakowi VLAN?

•Wyłącz negocjacje magistrali dla portów magistrali i ustawowo porty nieprądowe jako porty dostępu.

•Wyłącz STP na wszystkich portach nienarunkowych.
•Użyj VLAN 1 jako natywnej sieci VLAN na portach magistrali.
•Użyj enkapsulacji ISL na wszystkich łączach magistrali.

Jaki byłby główny powód, dla którego atakujący przeprowadziłby atak przepełnienia adresu MAC?

•tak, aby przełącznik przestał przekierowywać ruch
•aby legalni gospodarze nie mogli uzyskać adresu MAC
•aby atakujący mógł zobaczyć ramki przeznaczone dla innych hostów
•aby atakujący mógł wykonać dowolny kod na przełączniku

Jaka jest główna różnica między implementacją urządzeń IDS i IPS?
•IDS może negatywnie wpłynąć na przepływ pakietu, podczas gdy IPS nie może.
•IDS musi zostać wdrożony wraz z urządzeniem zapory ogniowej, podczas gdy IPS może zastąpić zaporę ogniową.
•IDS pozwoliłby na złośliwy ruch przed jego zaadresowaniem, podczas gdy IPS natychmiast go zatrzymuje.
•IDS wykorzystuje technologię opartą na sygnaturach do wykrywania złośliwych pakietów, podczas gdy IPS wykorzystuje technologię opartą na profilu.
Który atak jest zdefiniowany jako próba wykorzystania luk w oprogramowaniu, które są nieznane lub nieujawnione przez dostawcę?

•zero dni
•Koń trojański
•brutalna siła
•człowiek w środku

Jakie są trzy poziomy podpisu dostarczone przez Snort IPS w ISR serii 4000? (Wybierz trzy.)

•bezpieczeństwo
•kropla
•odrzucić
•łączność
•sprawdzić
•zrównoważony

Jakie są trzy atrybuty podpisów IPS? (Wybierz trzy.)
•akcja
•długość
•wyzwalacz
•typ
•głębokość
•funkcja

Które dwie funkcje są zawarte zarówno w protokołach TACACS +, jak i RADIUS? (Wybierz dwa.)
•Obsługa SIP
•szyfrowanie hasła
•Obsługa 802.1X
•oddzielne procesy uwierzytelniania i autoryzacji
•wykorzystanie protokołów warstwy transportowej

Jaką funkcję zapewnia protokół RADIUS?

•RADIUS zapewnia szyfrowanie pełnego pakietu podczas przesyłania.
•RADIUS zapewnia osobne usługi AAA.
•RADIUS zapewnia osobne porty do autoryzacji i rachunkowości.
•RADIUS zapewnia bezpieczną komunikację za pomocą portu TCP 49.

Jakie są trzy cechy protokołu RADIUS? (Wybierz trzy.)

•wykorzystuje port TCP 49
•wykorzystuje porty UDP do uwierzytelniania i rachunkowości
•obsługuje 802.1X i SIP
•oddziela procesy uwierzytelniania i autoryzacji
•szyfruje całą treść pakietu
•jest otwartym standardowym protokołem AAA RFC

Która strefa zapory opartej na strefach jest zdefiniowana przez system i dotyczy ruchu przeznaczonego dla routera lub pochodzącego z routera?

•strefa lokalna
•strefa wewnętrzna
•strefa samoobsługowa
•strefa systemowa
•strefa zewnętrzna

Jakie są dwie zalety korzystania z ZPF zamiast klasycznej zapory ogniowej? (Wybierz dwa.)

•ZPF umożliwia umieszczanie interfejsów w strefach w celu kontroli IP.
•ZPF nie jest zależny od ACL.
•ZPF stosuje się wiele działańkontrolnych.
•Zasady ZPF są łatwe do odczytania i rozwiązywania problemów.
•W przypadku ZPF router zezwala na pakiety, chyba że zostaną wyraźnie zablokowane.

W jaki sposób zapora ogniowa obsługuje ruch, gdy pochodzi z sieci prywatnej i podróżuje do sieci DMZ?

•Ruch jest selektywnie odrzucany na podstawie wymagań serwisowych.
•Ruch jest zwykle dozwolony z niewielkimi lub żadnymi ograniczeniami.
•Ruch jest selektywnie dozwolony i kontrolowany.
•Ruch jest zwykle blokowany.

Które dwa protokoły generują informacje o połączeniu w tabeli stanu i są obsługiwane do stanowego filtrowania? (Wybierz dwa.)

•ICMP
•UDP
•DHCP
•TCP
•HTTP

Który typ zapory jest obsługiwany przez większość routerów i jest najłatwiejszy do wdrożenia?

•zapora nowej generacji
•bezstanowa zapora ogniowa

•stanowa zapora ogniowa
•zapora proxy

Jakiego narzędzia do testowania sieci użyłby administrator do oceny i weryfikacji konfiguracji systemu pod kątem zasad bezpieczeństwa i standardów zgodności?

•Tripwire
•L0phtcrack
•Nessus
•Metasploit

Jaki typ testu bezpieczeństwa sieci może wykryć i zgłosić zmiany wprowadzone w systemach sieciowych?

•skanowanie podatności
•skanowanie sieciowe
•sprawdzanie integralności
•testy penetracyjne

Jakie narzędzie do testowania bezpieczeństwa sieci ma możliwość podania szczegółów na temat źródła podejrzanej aktywności sieci?

•SIEM
•SuperScan
•Zenmap
•Tripwire

Jak współcześni kryptografowie bronią się przed atakami brutalnej siły?

•Użyj analizy statystycznej, aby wyeliminować najczęstsze klucze szyfrowania.

•Użyj przestrzeni klawiszy na tyle dużej, że przeprowadzenie udanego ataku zajmuje zbyt dużo pieniędzy i zbyt dużo czasu.

•Użyj algorytmu, który wymaga od atakującego zarówno tekstu zaszyfrowanego, jak i tekstu jawnego, aby przeprowadzić udany atak.
•Użyj analizy częstotliwości, aby upewnić się, że najpopularniejsze litery używane w języku nie są używane w komunikacie szyfrującym.

Jak działa szyfr Cezara na wiadomości?

•Listy wiadomości są zastępowane inną literą, która jest ustaloną liczbą miejsc w alfabecie.
•Listy wiadomości są losowo układane.
•Listy wiadomości są uporządkowane w oparciu o z góry określony wzór.
•Słowa wiadomości są zastępowane na podstawie z góry określonego wzorca.

Jaki jest główny czynnik zapewniający bezpieczeństwo szyfrowania nowoczesnych algorytmów?
•złożoność algorytmu skrótu
•zastosowanie 3DES w stosunku do AES
•tajemnica kluczy

•tajemnica algorytmu

Jaki jest następny krok w ustanowieniu sieci VPN IPsec po zakończeniu fazy 1 IKE?

•negocjacje polityki ISAKMP
•negocjacje w sprawie polityki IPsec SA
•wykrywanie interesującego ruchu
•uwierzytelnianie rówieśników

Który algorytm może zapewnić integralność danych?
•RSA
•AES
•MD5
•PKI

Firma wdraża politykę bezpieczeństwa, która zapewnia, że plik wysyłany z centrali do oddziału może być otwierany tylko z ustalonym kodem. Ten kod jest zmieniany każdego dnia. Których dwóch algorytmów można użyć do wykonania tego zadania? (Wybierz dwa.)

•HMAC
•MD5
•3DES
•SHA-1
•AES

Technik sieci został poproszony o zaprojektowanie wirtualnej sieci prywatnej między dwoma routerami odgałęzionymi. Jakiego rodzaju klucza kryptograficznego należy użyć w tym scenariuszu?

•klucz skrótu
•klucz symetryczny
•klucz asymetryczny
•podpis cyfrowy

Które dwie opcje mogą ograniczyć informacje wykryte podczas skanowania portów? (Wybierz dwa.)

•system zapobiegania włamaniom
•zapora ogniowa
•uwierzytelnianie
•hasła
•szyfrowanie

Administrator odkrywa, że użytkownik uzyskuje dostęp do nowo utworzonej strony internetowej, która może być szkodliwa dla bezpieczeństwa firmy. Jakie działania powinien podjąć administrator w zakresie polityki bezpieczeństwa?

•Poproś użytkownika o natychmiastowe zatrzymanie się i poinformowanie użytkownika, że stanowi to podstawę do zwolnienia.
•Utwórz regułę zapory blokującą odpowiednią stronę internetową.
•Natychmiast zmień AUP i poproś wszystkich użytkowników o podpisanie zaktualizowanego AUP.
•Natychmiast zawiesić uprawnienia sieciowe użytkownika
.

ACL są używane przede wszystkim do filtrowania ruchu. Jakie są dwa dodatkowe zastosowania ACL? (Wybierz dwa.):

•określanie wewnętrznych hostów dla NAT

•identyfikacja ruchu dla QoS
•określanie adresów źródłowych do uwierzytelnienia
•reorganizacja ruchu do sieci VLAN
•filtrowanie pakietów VTP

Jakie dwie funkcje zostały dodane w SNMPv3 w celu usunięcia słabości poprzednich wersji SNMP? (Wybierz dwa.)

•uwierzytelnianie
•autoryzacja z priorytetem łańcucha społeczności
•masowe wyszukiwanie obiektów MIB
•Filtrowanie zarządzania ACL
•szyfrowanie

Jakie narzędzie do testowania sieci jest używane do audytu i odzyskiwania hasła?
•Nessus
•Metasploit
•L0phtcrack
•SuperScan

Jaki typ zapory wykorzystuje serwer do łączenia się z urządzeniami docelowymi w imieniu klientów?

•zapora filtrująca pakiety
•zapora proxy
•bezstanowa zapora ogniowa
•stanowa zapora ogniowa
Które dwa stwierdzenia opisują cechy algorytmów symetrycznych? (Wybierz dwa.)

•Są powszechnie używane w ruchu VPN.
•Używają pary klucza publicznego i klucza prywatnego.
•Są one powszechnie implementowane w protokołach SSL i SSH.
•Zapewniają poufność, integralność i dostępność.
•Są one określane jako wstępnie udostępniony klucz lub tajny klucz.
Administrator serwera WWW konfiguruje ustawienia dostępu, aby wymagać od użytkowników uprzedniego uwierzytelnienia przed uzyskaniem dostępu do niektórych stron internetowych. Który wymóg bezpieczeństwa informacji jest spełniony poprzez konfigurację?

•dostępność
•integralność
•skalowalność
•poufność

Zastosowanie 3DES w ramach IPsec jest przykładem tego, który z pięciu bloków konstrukcyjnych IPsec?

•uwierzytelnianie
•brak odrzucenia
•integralność
•Diffie-Hellman
•poufność

Jaką funkcję zapewnia Snort jako część Cebuli Bezpieczeństwa?

•generowanie alertów włamań do sieci za pomocą reguł i podpisów
•w celu normalizacji dzienników z różnych dzienników danych NSM, aby można je było reprezentować, przechowywać i uzyskiwać do nich dostęp za pomocą wspólnego schematu
•do wyświetlania przechwytywania pełnego pakietu do analizy
•do przeglądania transkryptów pcap generowanych przez narzędzia do wykrywania włamań

Jakie są dwie wady korzystania z HIPS? (Wybierz dwa.) •W przypadku HIPS

nie można łatwo ustalić powodzenia lub niepowodzenia ataku.

•W przypadku HIPS administrator sieci musi zweryfikować obsługę wszystkich różnych systemów operacyjnych używanych w sieci.
•HIPS ma trudności z konstruowaniem dokładnego obrazu sieci lub koordynowaniem zdarzeń, które występują w całej sieci.
•Jeśli strumień ruchu sieciowego jest zaszyfrowany, HIPS nie może uzyskać dostępu do niezaszyfrowanych formularzy ruchu.
•Instalacje HIPS są podatne na ataki fragmentacyjne lub zmienne ataki TTL.

W sieci z obsługą AAA użytkownik wydaje polecenie configure terminal z uprzywilejowanego trybu działania. Jaka funkcja AAA działa, jeśli to polecenie zostanie odrzucone?

•autoryzacja
•uwierzytelnianie
•audyt
•księgowość
Firma ma serwer plików, który udostępnia folder o nazwie Public. Polityka bezpieczeństwa sieci określa, że folder publiczny ma przypisane prawa tylko do odczytu każdemu, kto może zalogować się do serwera, podczas gdy prawa do edycji są przypisane tylko do grupy administratorów sieci. Który komponent jest adresowany w ramach usług sieciowych AAA?

•automatyzacja
•księgowość
•uwierzytelnianie
•autoryzacja

Co jest charakterystyczne dla strefy DMZ?

•Ruch pochodzący z sieci wewnętrznej przechodzącej do sieci DMZ jest

niedozwolony.

•Ruch pochodzący z sieci zewnętrznej przechodzący do sieci DMZ jest selektywnie dozwolony.
•Dozwolony jest ruch pochodzący z sieci DMZ przechodzącej do sieci wewnętrznej.
•Ruch pochodzący z sieci wewnętrznej przechodzącej do sieci DMZ jest selektywnie dozwolony.

Jaki środek może podjąć analityk bezpieczeństwa, aby przeprowadzić skuteczne monitorowanie bezpieczeństwa ruchu sieciowego szyfrowanego technologią SSL?

•Użyj serwera Syslog do przechwytywania ruchu sieciowego.
•Wdróż urządzenie Cisco SSL.
•Wymagaj połączeń zdalnego dostępu przez IPsec VPN.
•Wdróż Cisco ASA.

Jakie środki bezpieczeństwa są skuteczne w zapobieganiu atakom przepełnienia stołu CAM?

•Szpiegowanie DHCP
•Dynamiczna kontrola ARP
•Ochrona źródła IP
•ochrona portu

Jakie są dwa przykłady ataków DoS? (Wybierz dwa.)

•skanowanie portów
•Wstrzyknięcie SQL
•ping śmierci
•phishing
•przepełnienie bufora

Którą metodę stosuje się do identyfikacji interesującego ruchu potrzebnego do utworzenia tunelu IKE fazy 1?

•zestawy transformacyjne
•wpis listy dostępu do pozwolenia
•algorytmy skrótu
•stowarzyszenie bezpieczeństwa

Kiedy CLI jest używany do skonfigurowania ISR dla połączenia VPN między witrynami, które dwa elementy muszą zostać określone, aby włączyć zasady mapy kryptograficznej? (Wybierz dwa.)

•hash
•rówieśnik
•szyfrowanie
•polityka ISAKMP
•poprawna lista dostępu
•Adresy IP wszystkich aktywnych interfejsów
•zasady IKE Phase 1

W jaki sposób zapora ogniowa obsługuje ruch, gdy pochodzi z sieci publicznej i podróżuje do sieci DMZ?

•Ruch pochodzący z sieci publicznej jest kontrolowany i selektywnie dozwolony podczas podróży do sieci DMZ.
•Ruch pochodzący z sieci publicznej jest zwykle dozwolony z niewielkimi lub żadnymi ograniczeniami podczas podróży do sieci DMZ.
•Ruch pochodzący z sieci publicznej jest zwykle przesyłany bez kontroli podczas podróży do sieci DMZ.
•Ruch pochodzący z sieci publicznej jest zwykle blokowany podczas podróży do sieci DMZ.

Klient łączy się z serwerem WWW. Który element tego połączenia HTTP nie jest badany przez stanową zaporę ogniową?

•źródłowy adres IP ruchu klienta
•numer portu docelowego ruchu klienta
•rzeczywista zawartość połączenia HTTP
•numer portu źródłowego ruchu klienta

Która technologia monitorowania sieci wykorzystuje sieci VLAN do monitorowania ruchu na zdalnych przełącznikach?

•IPS
•IDS
•TAP
•RSPAN

Które działanie reguły spowoduje, że Snort IPS zablokuje i zarejestruje pakiet? •dziennik

•kropla
•alarm
•Sdrop

Co jest zwykle używane do stworzenia pułapki bezpieczeństwa w obiekcie centrum danych?

•Identyfikatory, dane biometryczne i dwoje drzwi dostępu
•monitory wysokiej rozdzielczości
•nadmiarowe serwery uwierzytelniające
•serwer bez wszystkich zastosowanych poprawek bezpieczeństwa

Firma zajmuje się wyciekiem i kradzieżą danych korporacyjnych w formie papierowej. Która technika ograniczania utraty danych może pomóc w tej sytuacji?

•silne ustawienia bezpieczeństwa komputera
•silne hasła
•niszczenie
•szyfrowanie

Po ukończeniu kursu bezpieczeństwa sieci student decyduje się na karierę w kryptoanalizie. Jaką pracę wykonałby student jako kryptoanalityk?

•łamanie kodu bez dostępu do wspólnego tajnego klucza
•tworzenie kodów skrótu w celu uwierzytelnienia danych
•tworzenie i łamanie tajnych kodów
•tworzenie szyfrów transpozycyjnych i substytucyjnych

Jakie są dwie wady korzystania z IDS? (Wybierz dwa.)

•IDS nie zatrzymuje złośliwego ruchu.
•IDS działa offline przy użyciu kopii ruchu sieciowego.
•IDS nie ma wpływu na ruch uliczny.
•IDS analizuje rzeczywiste przekazane pakiety.
•IDS wymaga, aby inne urządzenia reagowały na ataki.

Jakie porty mogą odbierać przesyłany ruch z izolowanego portu, który jest częścią sieci PVLAN?

•inne izolowane porty i porty społeczności
•tylko porty rozwiązłe
•wszystkie inne porty w tej samej społeczności
•tylko izolowane porty

Użytkownik skarży się na zablokowanie urządzenia po zbyt wielu nieudanych próbach logowania AAA. Co może być wykorzystane przez administratora sieci do zapewnienia bezpiecznej metody dostępu do uwierzytelniania bez blokowania użytkownika poza urządzeniem?

•Użyj polecenia opóźnienia logowania do prób uwierzytelnienia.

•Użyj lokalnego polecenia logowania, aby uwierzytelnić dostęp użytkownika.
•Użyj polecenia aaa lokalne uwierzytelnianie próbuje maksymalnego niepowodzenia globalnego trybu konfiguracji z większą liczbą akceptowalnych awarii.
•Podczas konfigurowania listy metod uwierzytelniania użyj słowa kluczowego brak.

Jakie są dwie wady przypisywania poziomów uprawnień użytkownika routerowi Cisco? (Wybierz dwa.)

•Tylko użytkownik root może dodawać lub usuwać polecenia.
•Poziomy uprawnień muszą być ustawione, aby umożliwić kontrolę dostępu do określonych interfejsów urządzeń, portów lub gniazd.
•Przypisanie polecenia z wieloma słowami kluczowymi umożliwia dostęp do wszystkich poleceń za pomocą tych słów kluczowych.
•Polecenia z niższego poziomu są zawsze wykonywalne na wyższym poziomie.
•AAA musi być włączone.

Jakie są dwa powody, aby włączyć uwierzytelnianie protokołu routingu OSPF w sieci? (Wybierz dwa.)

•aby zapobiec przekierowaniu, a następnie odrzuceniu ruchu danych
•w celu zapewnienia szybszej konwergencji sieci
•zapewnienie bezpieczeństwa danych poprzez szyfrowanie
•aby zapobiec przekierowaniu ruchu danych do niepewnego łącza
•w celu zapewnienia bardziej wydajnego routingu

Jakie trzy funkcje zapewnia usługa rejestrowania syslog? (Wybierz trzy.)

•zbieranie informacji o logowaniu
•uwierzytelnianie i szyfrowanie danych wysyłanych przez sieć
•zatrzymywanie przechwyconych wiadomości na routerze po ponownym uruchomieniu routera
•określając, gdzie przechowywane są przechwycone informacje
•rozróżnienie między informacjami do przechwycenia a informacjami do zignorowania
•ustawienie rozmiaru bufora rejestrowania

Jakie dwa typy komunikatów ICMPv6 muszą być dozwolone za pośrednictwem list kontroli dostępu IPv6, aby umożliwić rozdzielczość adresów warstwy 3 na adresy MAC warstwy 2? (Wybierz dwa.)

•pozyskiwanie sąsiadów
•żądania echa
•reklamy sąsiadów
•odpowiedzi echa
•pozyskiwanie routera
•reklamy routera

Jakie trzy usługi są świadczone za pośrednictwem podpisów cyfrowych? (Wybierz trzy.)
•księgowość
•autentyczność
•kompresja
•brak odrzucenia
•integralność
•szyfrowanie

Technik ma udokumentować bieżące konfiguracje wszystkich urządzeń sieciowych w college'u, w tym w budynkach zewnętrznych. Którego protokołu najlepiej użyć, aby bezpiecznie uzyskać dostęp do urządzeń sieciowych?

•FTP
•HTTP
•SSH
•Telnet

Administrator próbuje opracować politykę bezpieczeństwa BYOD dla pracowników, którzy wprowadzają szeroką gamę urządzeń do połączenia z siecią firmy. Do jakich trzech celów musi odnosić się polityka bezpieczeństwa BYOD? (Wybierz trzy.)

•Wszystkie urządzenia muszą być ubezpieczone od odpowiedzialności, jeśli zostaną wykorzystane do naruszenia sieci korporacyjnej.
•Wszystkie urządzenia muszą mieć otwarte uwierzytelnianie w sieci korporacyjnej.
•Prawa i działania dozwolone w sieci korporacyjnej muszą zostać określone.
•Należy wprowadzić zabezpieczenia przed zagrożeniem dla każdego urządzenia osobistego.
•Należy określić poziom dostępu pracowników podczas łączenia się z siecią korporacyjną.
•Wszystkie urządzenia powinny mieć możliwość bezbłędnego podłączenia do sieci korporacyjnej.

Jaka jest funkcja transmisji w zaporze opartej na strefie Cisco IOS?
•rejestrowanie odrzuconych lub upuszczonych pakietów
•kontrola ruchu między strefami w celu kontroli ruchu
•śledzenie stanu połączeń między strefami
•przekazywanie ruchu z jednej strefy do drugiej

Jakiego narzędzia do testowania sieci można użyć do identyfikacji protokołów warstwy sieciowej działających na hoście?

•SIEM
•Nmap
•L0phtcrack
•Tripwire

Czy we wdrażaniu zabezpieczeń na wielu urządzeniach ASA ACL różnią się od Cisco IOS ACL?
•Routery Cisco IOS wykorzystują zarówno nazwane, jak i numerowane listy ACL, a urządzenia Cisco ASA wykorzystują tylko numerowane listy ACL.
•Cisco IOS ACL są skonfigurowane z maską wieloznaczną, a Cisco ASA ACL są skonfigurowane z maską podsieci.
•ACL Cisco IOS są przetwarzane sekwencyjnie od góry do dołu, a ACL Cisco ASA nie są przetwarzane sekwencyjnie.
•Cisco IOS ACL wykorzystują niejawne zaprzeczenie wszystkim, a Cisco ASA ACL kończą się niejawnym zezwoleniem wszystkim.

Które stwierdzenie opisuje ważną cechę VPN między witrynami?

•Musi być ustawiony statycznie.
•Idealnie nadaje się do użytku przez pracowników mobilnych.
•Wymaga użycia klienta VPN na komputerze hosta.

•Po ustanowieniu początkowego połączenia może dynamicznie zmieniać informacje o połączeniu.
•Jest powszechnie wdrażany przez sieci dialup i modemów kablowych.

Które dwie opcje to najlepsze praktyki bezpieczeństwa, które pomagają zmniejszyć ryzyko BYOD? (Wybierz dwa.)

•Używaj farby, która odbija sygnały bezprzewodowe i szkła, które zapobiegają wydostawaniu się sygnałów na zewnątrz budynku.
•Aktualizuj system operacyjny urządzenia i oprogramowanie.
•Zezwalaj tylko na urządzenia zatwierdzone przez korporacyjny zespół IT.
•Włącz Wi-Fi tylko podczas korzystania z sieci bezprzewodowej.
•Zmniejsz poziom wzmocnienia anteny bezprzewodowej.
•Użyj bezprzewodowego filtrowania adresów MAC.

Niedawno utworzony ACL nie działa zgodnie z oczekiwaniami. Administrator ustalił, że ACL został zastosowany w interfejsie i to był niepoprawny kierunek. Jak administrator powinien rozwiązać ten problem?

•Usuń oryginalną ACL i utwórz nową ACL, stosując ją wychodzącą na interfejsie.
•Dodaj powiązanie wyjścia ACL na tym samym interfejsie.
•Napraw instrukcje ACE, aby działały zgodnie z oczekiwaniami w interfejsie.
•Usuń skojarzenie przychodzące ACL na interfejsie i ponownie zastosuj je wychodzące.

Jaka cecha subskrypcji opartych na snortach dotyczy zarówno społeczności, jak i zestawów reguł subskrybentów?

•Oba mają 30-dniowy opóźniony dostęp do zaktualizowanych podpisów.
•Oba wykorzystują Cisco Talos do zapewnienia zasięgu przed exploitami.
•Oba są w pełni obsługiwane przez Cisco i obejmują obsługę klienta Cisco.
•Oba zapewniają ochronę przed zagrożeniami bezpieczeństwa.

Analityk bezpieczeństwa konfiguruje Snort IPS. Analityk właśnie pobrał i zainstalował plik Snort OVA. Jaki jest następny krok?

•Sprawdź Snort IPS.
•Skonfiguruj interfejsy grupy portów wirtualnych.
•Włącz IPS globalnie lub na pożądanych interfejsach.
•Aktywuj usługi wirtualne.

Polityka bezpieczeństwa w firmie określa, że stacje robocze pracowników mogą inicjować połączenia HTTP i HTTPS z zewnętrznymi stronami internetowymi, a ruch powrotny jest dozwolony. Jednak połączenia inicjowane z zewnętrznych hostów są niedozwolone. Który parametr można zastosować w rozszerzonych ACL, aby spełnić to wymaganie?

•dscp
•pierwszeństwo
•ekwiwalent
•ustanowiony

Badacz porównuje różnice między bezstanową zaporą ogniową a zaporą proxy. Które dwie dodatkowe warstwy modelu OSI są sprawdzane przez zaporę proxy? (Wybierz dwa.)

•Warstwa 3
•Warstwa 4

•Warstwa 5
•Warstwa 6
•Warstwa 7

Który poziom uprawnień ma największy dostęp do Cisco IOS?

•poziom 0
•poziom 15
•poziom 7
•poziom 16
•poziom 1

Analityk sieci konfiguruje VPN IPsec między witrynami. Analityk skonfigurował zarówno zasady ISAKMP, jak i IPsec. Jaki jest następny krok

? •Skonfiguruj skrót jako SHA, a uwierzytelnianie jako wstępnie udostępnione.

•Zastosuj mapę kryptograficzną do odpowiednich interfejsów wychodzących.
•Wydaj polecenie crypto ipsec sa, aby zweryfikować tunel.
•Sprawdź, czy funkcja bezpieczeństwa jest włączona w systemie IOS.

Kiedy wdrażany jest przychodzący ACL ruchu internetowego, co należy uwzględnić, aby zapobiec fałszowaniu sieci wewnętrznych?

•ACE zapobiegają ruchowi z prywatnych przestrzeni adresowych
•ACE zapobiegające ruchowi adresów rozgłoszeniowych
•ACE zapobiegające ruchowi ICMP
•ACE zapobiegają ruchowi HTTP •ACE zapobiegają ruchowi SNMP **akie dwa rodzaje ataków są przykładami ataków rozpoznawczych? (Wybierz dwa.)**

•brutalna siła
•skanowanie portu
•ping sweter
•człowiek w środku
•Powódź SYN

Które rozwiązanie Cisco pomaga zapobiegać fałszowaniu ARP i atakom zatrucia ARP?

•Dynamiczna kontrola ARP
•Ochrona źródła IP
•DHCP Snooping
•Bezpieczeństwo portu

Kiedy urządzenie Cisco NAC ocenia połączenie przychodzące ze zdalnego urządzenia na podstawie zdefiniowanych zasad sieciowych, jaka funkcja jest używana?

•ocena postawy
•rekultywacja systemów niezgodnych
•uwierzytelnianie i autoryzacja
•kwarantanna systemów niezgodnych

Jakie dwa kroki są wymagane, aby włączyć SSH na routerze Cisco? (Wybierz dwa.)

•Nadaj routerowi nazwę hosta i nazwę domeny.

•Utwórz baner, który będzie wyświetlany użytkownikom podczas łączenia.
•Generuj zestaw tajnych kluczy, które będą używane do szyfrowania i deszyfrowania.
•Skonfiguruj serwer uwierzytelniania do obsługi żądań połączenia przychodzącego.
•Włącz SSH na fizycznych interfejsach, na których będą odbierane przychodzące żądania połączenia.

Administrator sieci witryny e-commerce wymaga usługi, która uniemożliwia klientom twierdzenie, że legalne zamówienia są fałszywe. Jaka usługa zapewnia tego rodzaju gwarancję?

•poufność
•uwierzytelnianie
•integralność
•brak odrzucenia

Jakie funkcje zapewnia Cisco SPAN w przełączanej sieci?

•Odzwierciedla ruch, który przechodzi przez port przełączania lub VLAN do innego portu w celu analizy ruchu.
•Zapobiega zakłóceniu ruchu w sieci LAN przez burzę nadawczą.
•Chroni przełączaną sieć przed odbieraniem BPDU na portach, które nie powinny ich odbierać.
•Kopiuje ruch przechodzący przez interfejs przełącznika i wysyła dane bezpośrednio do syslog lub serwera SNMP w celu analizy.
•Sprawdza protokoły głosowe, aby upewnić się, że żądania SIP, SCCP, H.323 i MGCP są zgodne ze standardami głosowymi.
•Łagodzi ataki przepełnienia adresu MAC.

Które trzy stwierdzenia są ogólnie uważane za najlepsze praktyki w zakresie umieszczania ACL? (Wybierz trzy.)

•Filtruj niechciany ruch, zanim przejdzie do łącza o niskiej przepustowości.
•Umieść standardowe listy ACL w pobliżu docelowego adresu IP ruchu.
•Umieść standardowe listy ACL w pobliżu źródłowego adresu IP ruchu.
•Umieść rozszerzone ACL w pobliżu docelowego adresu IP ruchu.
•Umieść rozszerzone ACL w pobliżu źródłowego adresu IP ruchu.
•Dla każdego przychodzącego ACL umieszczonego na interfejsie powinna istnieć pasująca wychodząca ACL.

Jaką funkcję pełni obiekt konfiguracyjny map klas w modułowej strukturze zasad Cisco?

•identyfikacja interesującego ruchu
•stosowanie zasad do interfejsu
•stosowanie zasad do interesującego ruchu
•ograniczanie ruchu przez interfejs

Próbując zapobiec atakom sieciowym, analitycy cyber dzielą się z kolegami unikalnymi możliwymi do zidentyfikowania atrybutami znanych ataków. Jakie trzy rodzaje atrybutów lub wskaźników kompromisu są pomocne do udostępnienia? (Wybierz trzy.)

•Adresy IP serwerów atakujących
•zmiany wprowadzone w oprogramowaniu końcowym
•nazwy netbios skompromitowanych zapór ogniowych
•funkcje złośliwego oprogramowania

•BIOS systemów atakujących
•identyfikator systemu zagrożonych systemów

Jakie dwa zapewnienia zapewnia podpisywanie cyfrowe dotyczące kodu pobieranego z Internetu? (Wybierz dwa.)

•Kod jest autentyczny i faktycznie pochodzi od wydawcy.
•Kod nie zawiera błędów.
•Kod nie został zmodyfikowany, ponieważ opuścił wydawcę oprogramowania.
•Kod nie zawiera wirusów.
•Kod został zaszyfrowany zarówno kluczem prywatnym, jak i publicznym.

Które dwie instrukcje opisują użycie algorytmów asymetrycznych? (Wybierz dwa.)

•Klucze publiczne i prywatne mogą być używane zamiennie.
•Jeśli do szyfrowania danych używany jest klucz publiczny, do odszyfrowania danych należy użyć klucza publicznego.
•Jeśli do szyfrowania danych używany jest klucz prywatny, do odszyfrowania danych należy użyć klucza publicznego.
•Jeśli do szyfrowania danych używany jest klucz publiczny, do odszyfrowania danych należy użyć klucza prywatnego.
•Jeśli do szyfrowania danych używany jest klucz prywatny, do odszyfrowania danych należy użyć klucza prywatnego.

Które stwierdzenie jest cechą HMAC?

•HMAC używa tajnego klucza, który jest znany tylko nadawcy i pokonuje ataki typu man-in-the-middle.
•HMAC używa protokołów takich jak SSL lub TLS, aby zapewnić poufność warstwy sesji.
•HMAC używa tajnego klucza jako wejścia do funkcji skrótu, dodając uwierzytelnienie do zapewnienia integralności.
•HMAC opiera się na funkcji skrótu RSA.

Jaki jest cel ACL typu w ASA?

•w celu sprawdzenia ruchu wychodzącego skierowanego w stronę niektórych stron internetowych
•ograniczenie ruchu przeznaczonego na ASDM
•do monitorowania ruchu powrotnego, który jest odpowiedzią na żądania serwera WWW inicjowane z interfejsu wewnętrznego
•filtrować ruch dla bez klienckich użytkowników SSL VPN

Który typ zapory jest najczęstszy i pozwala lub blokuje ruch na podstawie informacji o warstwie 3, warstwie 4 i warstwie 5?

•bezstanowa zapora ogniowa
•zapora filtrująca pakiety
•zapora nowej generacji
•stanowa zapora ogniowa

Którego protokołu lub środka należy użyć, aby złagodzić lukę w korzystaniu z FTP do przesyłania dokumentów między telepracownikiem a serwerem plików firmy?

•SCP
•TFTP

•ACL na serwerze plików
•pozapasmowy kanał komunikacyjny

Jakie narzędzie jest dostępne za pośrednictwem Cisco IOS CLI do inicjowania audytów bezpieczeństwa i wprowadzania zalecanych zmian konfiguracji z wejściem administratora lub bez niego?

•Kontrola kontroli samolotów
•Cisco AutoSecure
•Cisco ACS
•Prosty protokół zarządzania siecią

Które dwie technologie zapewniają rozwiązania VPN zarządzane przez przedsiębiorstwo? (Wybierz dwa.)

•Warstwa 3 MPLS VPN
•Przekaźnik ramy
•VPN od strony do strony
•Warstwa 2 MPLS VPN
•zdalny dostęp VPN

Jakie są trzy elementy identyfikatora mostu STP? (Wybierz trzy.)

•data i godzina wprowadzenia zmiany do sieci
•nazwa hosta przełącznika
•adres MAC przełącznika
•rozszerzony identyfikator systemu
•wartość priorytetowa mostu
•adres IP zarządzającej sieci VLAN

Jakie są dwie różnice między okazałymi i filtrującymi zapory ogniowe? (Wybierz dwa.)

•Zapora filtrująca pakiety zapobiegnie fałszowaniu, określając, czy pakiety należą do istniejącego połączenia, podczas gdy okazała zapora ogniowa przestrzega wstępnie skonfigurowanych zestawów reguł.
•Okazała zapora ogniowa zapewnia bardziej rygorystyczną kontrolę nad bezpieczeństwem niż zapora filtrująca pakiety.
•Zapora filtrująca pakiety może filtrować sesje wykorzystujące dynamiczne negocjacje portów, podczas gdy państwowa zapora ogniowa nie może.
•Okazała zapora sieciowa zapewni więcej informacji o rejestrowaniu niż zapora filtrująca pakiety.
•Zapora ogniowa sprawdzi każdy pakiet indywidualnie, a zapora filtrująca pakiet obserwuje stan połączenia.

Jaki stan portu jest używany przez 802.1X, jeśli stacja robocza nie autoryzuje?

•niepełnosprawny
•w dół
•nieautoryzowany
•blokowanie

Jakie dwie cechy dotyczą opartych na rolach przeglądów dostępu do CLI? (Wybierz dwa.)

•W konkretnym podglądzie nie można bezpośrednio dodawać do niego poleceń.
•Widoki CLI mają hasła, ale podglądy nie mają haseł.
•Pojedynczy podgląd może być udostępniany wielu widokom CLI.
•Usunięcie podglądu usuwa wszystkie powiązane widoki CLI.

•Użytkownicy zalogowani do podglądu mogą uzyskać dostęp do wszystkich poleceń określonych w powiązanych widokach CLI.

Jakie są dwie funkcje bezpieczeństwa powszechnie spotykane w projekcie WAN? (Wybierz dwa.)

•WPA2 do szyfrowania danych wszystkich danych między witrynami
•zapory ogniowe chroniące główne i odległe strony
•bezpieczeństwo poza obwodem, w tym ciągły nadzór wideo
•bezpieczeństwo portu we wszystkich portach skierowanych do użytkownika
•VPN używane przez pracowników mobilnych między witrynami