

kod szkolenia: SESA / PL AA 4d

Securing Email with Cisco Email Security Appliance

Szkolenie autoryzowane Cisco.

Płać punktami CLC:

Cisco Learning Credits accepted : 36 Credits per Class

Szczegóły i zapisy na stronie dostawcy:

<https://learninglocator.cloudapps.cisco.com/#/home>

Program Cisco Continuing Education to elastyczna oferta dedykowana dla wszystkich aktywnych osób posiadających certyfikaty na poziomie Associate, Specialist, Professional i Expert.

Dowiedz się więcej, jak możesz recertyfikować się w ramach CE, aby zachować aktywny status certyfikacji.

[Cisco Continuing Education Program - CE](#)

Uczestnictwo w autoryzowanym szkoleniu pozwala Ci uzyskać dodatkowe punkty potrzebne do utrzymania certyfikacji.

SESA: 24 punkty CE



Przeznaczenie szkolenia

Szkolenie skierowane jest dla osób planujących przeprowadzenie skutecznego procesu instalacji i późniejszej administracji oraz rozwiązywania problemów z urządzeniami Cisco Email Security Appliance.



Korzyści wynikające z ukończenia szkolenia

Kurs SESA pomaga przygotować się do certyfikacji Cisco® CCNP® Security i CCIE® Security oraz do pracy na stanowisku starszego inżyniera bezpieczeństwa teleinformatycznego. Na tym kursie opanujesz umiejętności i technologie potrzebne do wdrożenia produktu Cisco ESA. Dowiesz się w jaki sposób monitorować oraz rozwiązywać problemy z działaniem Cisco ESA.



Opis egzaminu

Szkolenie przygotowuje do egzaminu 300-720 SESA, który można zdawać za dodatkową opłatą w centrum PearsonVUE. Egzamin można również zdawać w formule on-line. Szczegóły dostępne są na stronie: <https://home.pearsonvue.com/cisco/onvue>



Oczekiwane przygotowanie słuchaczy

Dobra znajomość podstaw TCP/IP, adresacji IP, routingu, DNS, SSH, FTP, SNMP, http(s) oraz protokołu TCP

Doświadczenie z komunikacją internetową przy użyciu protokołu SMTP, użyciem formatów wiadomości (MIME)

Wiedza na poziomie szkoleń: CCNA, SCOR, SFNDU



Język szkolenia

- Szkolenie: polski
- Materiały: angielski



Czas trwania

4 dni / 28 godzin

Agenda szkolenia

1. Charakterystyka produktu Cisco ESA

- Przegląd rozwiązania Cisco ESA
- Przegląd produktów Cisco ESA
- Charakterystyka protokołu SMTP
- Scenariusze instalacji Cisco ESA
- Wstępna konfiguracja Cisco ESA
- Funkcjonalności dostępne w ramach systemu operacyjnego Async 11.x

2. Administrowanie Cisco ESA

- Dystrybucja poleceń administracyjnych
- Administracja systemem operacyjnym Cisco ESA
- Zaawansowana konfiguracja karty sieciowej Cisco ESA
- Śledzenie wiadomości e-mail oraz logowanie zdarzeń

3. Kontrolowanie domeny nadawcy oraz odbiorcy

- Publiczny i prywatny serwer E-mail
- Konfiguracja bramy do odbierania wiadomości E-mail
- Konfiguracja zaufanych serwerów E-mail
- Konfiguracja routingu dla wiadomości poczty elektronicznej

4. Kontrolowanie spamu z użyciem Cisco Talos SenderBase

- Przegląd rozwiązania SenderBase
- AntySpam
- Ochrona przed złośliwymi lub niechcianymi wiadomościami e-mail
- Filtrowanie na bazie reputacji pliku

5. Konfiguracja antywirusa i zewnętrznych filtrów

- Przegląd rozwiązania antywirus
- Wykrywanie wirusów z użyciem McAfee oraz Sophos
- Konfiguracja ESA do używania filtrów antywirusowych
- Działanie filtrów zewnętrznych

6. Zasady korzystania z poczty elektronicznej

- Przegląd managera ESA
- Przegląd zasad odnośnie wysyłania i odbierania e-mail
- Wdrażanie zasad dotyczących przetwarzania przychodzących i wychodzących wiadomości
- Sposoby dopasowania użytkownika do wdrożonych zasad przetwarzania e-mail

7. Używanie filtrów bazujących na treści e-mail

- Przegląd dostępnych filtrów bazujących na zawartości wiadomości
- Warunki oraz akcje dostępne w ramach filtrów
- Wykorzystanie słowników do filtrowania e-mail

8. Używanie filtrów bazujących na rodzaju wiadomości

- Przegląd filtrów bazujących na typie wiadomości
 - Komponenty filtra wiadomości
 - Przetwarzanie wiadomości przez filtr
 - Akcje związane z filtrem wiadomości
 - Skanowanie załączników
 - Konfiguracja filtrowania wiadomości na bazie zasady behawioralnej
9. Ochrona przed utratą danych
- Proces skanowania DLP
 - Wdrożenie oraz ustanowienie zasad skanowania DLP
 - Aktualizacja procesu DLP
10. Podłączenie Cisco ESA do LDAP
- Przegląd rozwiązania LDAP
 - Stosowanie zapytań do LDAP
 - Konfiguracja uwierzytelniania użytkowników względem LDAP
 - Sprawdzanie użytkowników E-mail względem LDAP
11. Uwierzytelnianie sesji do serwera SMTP
- Konfiguracja ESA do uwierzytelniania użytkowników
 - Uwierzytelnianie użytkowników z użyciem certyfikatów cyfrowych
 - Sprawdzanie poprawności certyfikatu klienta
 - Uwierzytelnianie użytkownika względem LDAP
 - Zestawianie bezpiecznego połączenia do ESA przy użyciu TLS
 - Listy unieważnionych certyfikatów
12. Uwierzytelnianie wiadomości e-mail
- Przegląd mechanizmów do uwierzytelniania wiadomości e-mail
 - Przegląd mechanizmów weryfikacji SPF oraz SIDF
 - Konfiguracja kluczy domenowych oraz sygnalizacji DKIM
 - Weryfikacja przychodzących wiadomości przy użyciu DKIM
 - Weryfikacja wiadomości przy użyciu DMARC
13. Szyfrowanie treści wiadomości e-mail
- Przegląd mechanizmów szyfrowania treści e-mail
 - Szyfrowanie wiadomości e-mail Sposoby określania wiadomości, które będą zaszyfrowane
 - Dołączanie nagłówka mechanizmu szyfrującego do treści wiadomości e-mail
 - Szyfrowanie komunikacji z innymi MTA
 - Utrzymanie certyfikatów cyfrowych do innych serwerów E-mail
14. Wykorzystanie funkcjonalności kwarantanny oraz mechanizmów dostarczania e-mail
- Charakterystyka kwarantanny oraz obsługi e-mail trafiających do kwarantanny
 - Konfiguracja scentralizowanej kwarantanny
 - Konfiguracja wiadomości wysyłanych do użytkowników w sytuacji, gdy wiadomość trafi do kwarantanny
 - Kwarantanna na bazie wirusów oraz naruszenia zasad bezpieczeństwa
15. Scentralizowane zarządzanie ESA z użyciem funkcjonalności klastra

- Przegląd mechanizmów dostępnych w ramach klastra ESA
- Tworzenie i dołączanie węzłów do klastra ESA
- Zarządzanie oraz komunikacja w ramach klastra
- Wgrywanie konfiguracji do klastra ESA
- Dobre praktyki inżynierskie związane z wdrożeniem klastra ESA

16. Testowanie oraz rozwiązywanie problemów z Cisco ESA

- Debugowanie przepływu wiadomości e-mail
- Rozwiązywanie problemów z działaniem sieci, serwera nadrzędnego, dostarczaniem wiadomości
- Reagowanie na alarmy
- Rozwiązywanie problemów ze sprzętem fizycznym
- Współpraca z serwisem technicznym Cisco