Szkolenie autoryzowane

Certified Stormshield Network Administrator (CSNA)

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie techniczne poświęcone urządzeniom do ochrony styku sieci firmowej z Internetem firmy STORMSHIELD.

Długość szkolenia

24 h (3 dni x 8 h)

Szkolenie i materiały w języku polskim.

Korzyści po szkoleniu:

Idealna propozycja szkolenia zarówno dla osób, które właśnie nabyły urządzenie Stormshield lub dla tych, którzy w praktyczny sposób chcą zapoznać się z możliwościami rozwiązania.

Biorąc udział w szkoleniu otrzymasz **bezpłatny dostęp do maszyn wirtualnych** po to, byś mógł po szkoleniu jeszcze raz wykonać wszystkie ćwiczenia realizowane podczas szkolenia lub lepiej przygotować się do egzaminu producenta.

Dodatkowo będziesz:

- sprawnie zarządzał urządzeniami Stormshield i wiedział jak one działają,
- potrafił wdrożyć urządzenie Stormshield w sieci firmowej,
- definiował polityki filtrowania (Firewall i NAT) oraz trasy routingu,
- kontrolował dostęp do stron internetowych (http i https),
- konfigurował polityki bezpieczeństwa dla uwierzytelnionych użytkowników,
- potrafił wdrożyć różne typy wirtualnych sieci prywatnych (VPN) - IPSec VPN i SSL VPN.

Wymagania:

- podstawowa znajomość konfiguracji sieci komputerowych,
- podstawowa znajomość zagadnień związanych z TCP/IP.

Program szkolenia

1. Przedstawienie uczestników
2. Program szkolenia i certyfikacje
3. Przedstawienie firmy Stormshield i jej produktów
4. Rozpoczęcie pracy z urządzeniem
   - Rejestracja w strefie klienta i dostęp zasobów
   - Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego
   - Ustawienia systemowe i uprawnienia administratorów
   - Instalacja licencji i aktualizacja systemu
   - Tworzenie kopii zapasowej i przywracanie konfiguracji
5. Zbieranie logów i monitorowanie
   - Przedstawienie kategorii zbieranych logów
   - Wykresy historyczne i monitorowanie
6. Obiekty
   - Typy obiektów oraz ich wykorzystanie
   - Obiekty sieciowe i obiekt typu „router”
7. Konfiguracja sieci
   - Tryby pracy urządzenia
   - Typy interfejsów (Ethernet, modem, bridge, VLAN, GRETAP)
   - Typy routingu oraz ich priorytety
8. Translacja adresów sieciowych (NAT)
9. Translacja połączeń wychodzących (maskarada)
10. Translacja połączeń przychodzących (przekierowanie)
11. Translacja dwukierunkowa (jeden do jeden)
12. Filtrowanie ruchu sieciowego (Firewall)

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł
Numer NIP: 634-012-60-68, numer REGON: 008173852

13. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)
    - Szczegółowy opis parametrów reguły Firewall
    - Kolejność przetwarzania reguł Firewall i NAT
14. Ochrona aplikacji
    - Implementacja filtrowania URL dla ruchu http i https
    - Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
    - Moduł IPS i stosowanie profili inspekcji
15. Użytkownicy i uwierzytelnianie
16. Konfiguracja usługi katalogowej
    - Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
    - Rejestracja użytkowników
    - Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania
17. Wirtualne sieci prywatne (VPN)
    - Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
    - Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
    - Tunele VTI
18. SSL VPN
    - Zasada działania
    - Konfiguracja

Tagi: