

Harmonogram szkolenia:

1. Informacje wprowadzające.

2. NETASQ – informacje o producencie.

3. Rozwiązania do zabezpieczenia sieci firmy NETASQ.

- Urządzenia NETASQ UTM serii „F”
- Urządzenia NETASQ UTM serii „U”
- Urządzenia NETASQ mFiltro
- Różnice pomiędzy serią „U” oraz serią „F”
- Oprogramowanie wewnętrzne (NS-BSD)
- Oprogramowanie zarządzające (Administration Suite)
- Zarządzanie z wykorzystaniem WebGUI

4. Pierwsze podłączenie do urządzenia NETASQ UTM.

- Omówienie podstawowej konfiguracji urządzenia
- Przywracanie urządzenia do ustawień fabrycznych
- Podłączenie do urządzenia poprzez interfejs Ethernet
- Podłączenie do urządzenia poprzez interfejs szeregowy (COM)
- Tworzenie kopii zapasowej konfiguracji
-

5. Tryby pracy urządzeń NETASQ UTM.

- Tryb transparent (bridge)
- Tryb advanced
- Tryb hybrid

6. Konfiguracja obiektów.

- Rola obiektów w konfiguracji urządzenia NETASQ UTM
- Dodawanie nowych obiektów
- Modyfikacja i usuwanie niepotrzebnych obiektów
- Konfiguracja obiektów czasu

7. Konfiguracja podstawowych usług urządzenia.

Konfiguracja usługi serwera DHCP

Konfiguracja usługi Proxy DNS

8. Polityki ochrony UTM

Rola zapór ogniowych w sieciach komputerowych

Przegląd prekonfigurowanych slotów z konfiguracją zapory sieciowej

Konfiguracja zapory sieciowej w urządzeniach NETASQ UTM

Grupowanie reguł oraz kontrola ich poprawności

Wstęp do Intrusion Prevention System

Konfiguracja IPS w urządzeniu NETASQ UTM

Konfiguracja trybów pracy filtrowania (IPS/IDS/Firewall)

9. Translacja adresów.

IPv4 i problem braku adresów IP

Dostępne tryby NAT w urządzeniach NETASQ UTM

Harmonogram i jego rola w translacji adresów IP

10. Autoryzacja użytkowników w oparciu o bazę danych.

Wprowadzenie do tematu autoryzacji użytkowników

Konfiguracja serwera LDAP w urządzeniu NETASQ UTM

Integracja urządzenia NETASQ z zewnętrzną bazą LDAP

Integracja urządzenia NETASQ z usługą Microsoft Active Directory

11. Mechanizm Captive Portal.

Wstęp do autoryzacji użytkowników poprzez przeglądarkę Web
Konfiguracja mechanizmu Captive Portal
Reguły zaporę ogniowej dla użytkowników zautoryzowanych

12. Wykorzystanie mechanizmu proxy dla najpopularniejszych usług.

Działanie mechanizmu proxy
Konfiguracja proxy http
Konfiguracja proxy SMTP/POP3
Konfiguracja Proxy FTP
Konfiguracja proxy SSL

13. Skanery.

Skaner antywirusowy
Konfiguracja skanera antywirusowego
Skaner antyspamowy
Konfiguracja skanera antyspamowego
Skaner filtra URL
Konfiguracja skanera filtra URL

14. Konfiguracja skanera podatności oprogramowania (Vulnerability Assessment)

Wprowadzenie do tematyki audytu sieci
Konfiguracja modułu
Przegląd informacji zgromadzonych przez skaner

15. Technologia VPN.

Wstęp do technologii VPN
Protokół PPTP
Kanały VPN typu client-to-site z wykorzystaniem protokołu PPTP
Protokół IPSec
Kanały VPN typu site-to-site z wykorzystaniem protokołu IPSec (PSK)
Kanały VPN typu client-to-site z wykorzystaniem protokołu IPSec (PSK)
SSL VPN

16. Logowanie zdarzeń.

Konfiguracja usługi syslog
Logowanie zdarzeń na zaporze
Analiza popularnych alarmów wykrytych przez urządzenie

17. Egzamin.