

Lp.	Nazwa komponentu	Wymagane minimalne parametry szkolenia
1	2	3
Certyfikowane szkolenie z zakresu dostarczonego rozwiązania		
1.	Typ	Certyfikowane szkolenie z zakresu zarządzania i administracji rozwiązaniem Firewall
2.	Czas trwania	3 dni
3.	Lokalizacja	<u>Szkolenie poza siedzibą klienta, na terenie Polski</u>
4.	Wymagany minimalny zakres tematyczny	<ol style="list-style-type: none"> <li>1. Rozpoczęcie pracy z urządzeniem <ul style="list-style-type: none"> <li>o Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego</li> <li>o Ustawienia systemowe i uprawnienia administratorów</li> <li>o Instalacja licencji i aktualizacja systemu</li> <li>o Tworzenie kopii zapasowej i przywracanie konfiguracji</li> </ul> </li> <li>2. Zbieranie logów i monitorowanie <ul style="list-style-type: none"> <li>o Przedstawienie kategorii zbieranych logów</li> <li>o Wykresy historyczne i monitorowanie</li> </ul> </li> <li>3. Obiekty <ul style="list-style-type: none"> <li>o Typy obiektów oraz ich wykorzystanie</li> <li>o Obiekty sieciowe i obiekt typu „router”</li> </ul> </li> <li>4. Konfiguracja sieci <ul style="list-style-type: none"> <li>o Tryby pracy urządzenia</li> <li>o Typy interfejsów (Ethernet, modem, bridge, VLAN, GRE/TAP)</li> <li>o Typy routingu oraz ich priorytety</li> </ul> </li> <li>5. Translacja adresów sieciowych (NAT)</li> <li>6. Translacja połączeń wychodzących (maskarada)</li> <li>7. Translacja połączeń przychodzących (przekierowanie)</li> <li>8. Translacja dwukierunkowa (jeden do jeden)</li> <li>9. Filtrowanie ruchu sieciowego (Firewall)</li> <li>10. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection) <ul style="list-style-type: none"> <li>o Szczegółowy opis parametrów reguły Firewall</li> <li>o Kolejność przetwarzania reguł Firewall i NAT</li> </ul> </li> <li>11. Ochrona aplikacji <ul style="list-style-type: none"> <li>o Implementacja filtrowania URL dla ruchu http i https</li> <li>o Konfigurowanie skanowania antywirusowego</li> <li>o Moduł IPS i stosowanie profili inspekcji</li> </ul> </li> <li>12. Użytkownicy i uwierzytelnianie</li> <li>13. Konfiguracja usługi katalogowej <ul style="list-style-type: none"> <li>o Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)</li> <li>o Rejestracja użytkowników</li> <li>o Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania</li> </ul> </li> <li>14. Wirtualne sieci prywatne (VPN)</li> </ol>

		<ul style="list-style-type: none"><li>○ Koncepcje i ogólne informacje dotyczące protokołu IPsec VPN (IKEv1 i IKEv2)</li><li>○ Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)</li><li>○ Tunele VTI</li></ul> <b>15. SSL VPN</b> <ul style="list-style-type: none"><li>○ Zasada działania</li><li>○ Konfiguracja</li></ul>
5.	<b>Egzamin</b>	Tak: Autoryzowany przez producenta egzamin.
6.	<b>Trenerzy</b>	Certyfikowani przez producenta rozwiązania Trenerzy
7.	<b>Materiały szkoleniowe</b>	Materiały elektroniczne, zgodne z wytycznymi producenta.