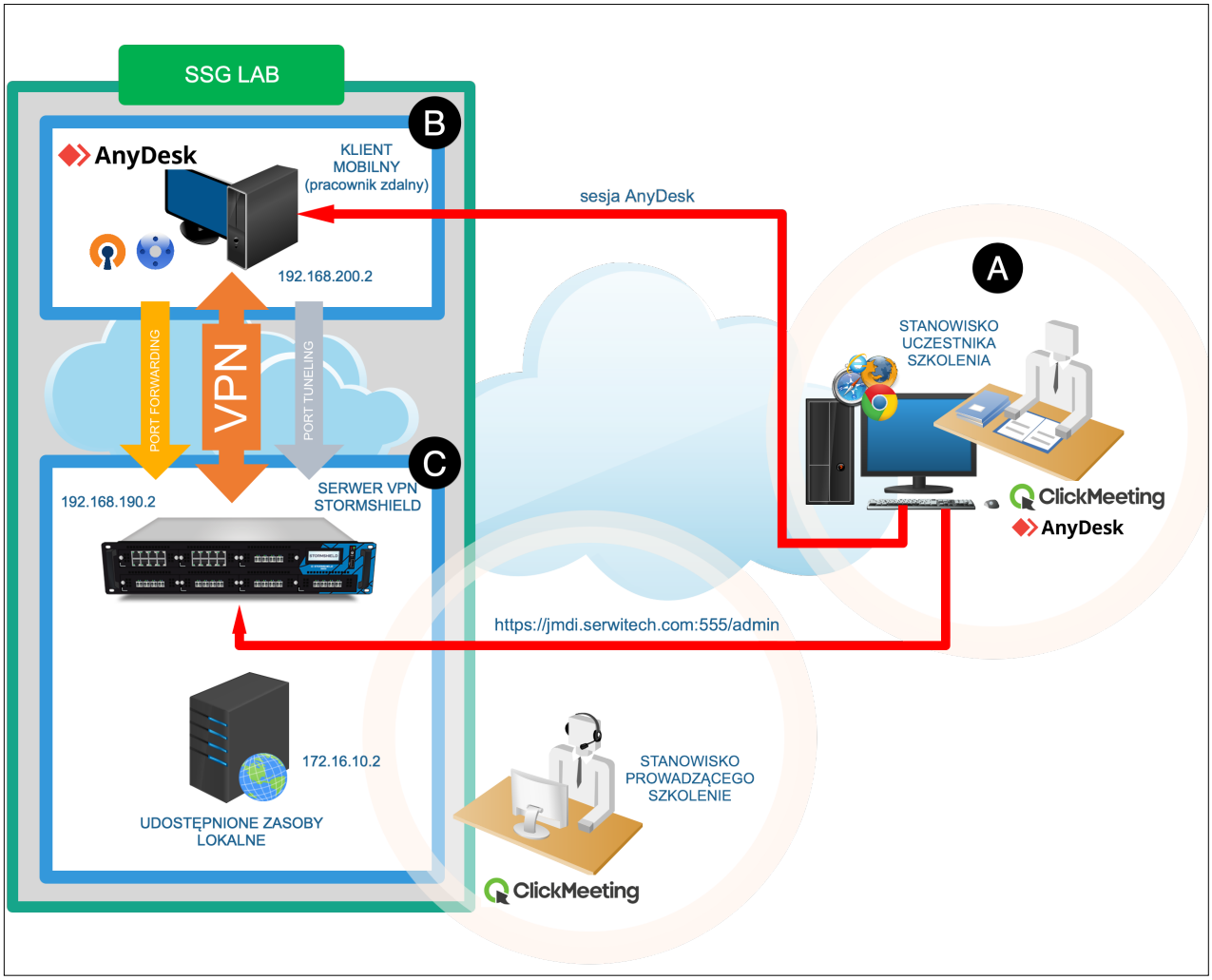

Praca zdalna (szkolenie)

instrukcja dostępu do zasobów

Autor: Paweł Grzelewski

Webinar: Praca zdalna - STORMSHIELD VPN

Data publikacji: 28.03.2020

OPIS STANOWISK

Stanowisko A

Komputer uczestnika szkolenia. Z poziomu tego komputera uczestnik szkolenia bierze udział w webinarze prowadzonym online z wykorzystaniem platformy **ClickMeeting**.
Webinar **Praca zdalna - STORMSHIELD VPN** jest dostępny pod adresem:
https://stormshield.clickmeeting.com/praca-zdalna-stormshield-vpn

Logowanie do webinara wymaga podania jednorazowego tokena dostarczanego przez organizatora szkolenia. Komputer powinien być wyposażony w kartę dźwiękową i mikrofon. Stosowanie kamerki internetowej jest możliwe ale nie jest to wymóg konieczny. Jeżeli istnieje taka możliwość wskazane jest użycie dodatkowego monitora lub drugiego komputera (jeden do komunikacji w ramach webinara, drugi do konfiguracji w ramach warsztatów praktycznych - dostęp do stanowisk **B** i **C**).
Należy pobrać oprogramowanie dostępu do pulpitu zdalnego **AnyDesk**. Oprogramowanie AnyDesk można zainstalować lub tylko uruchomić na czas szkolenia. Program jest dostępny do pobrania ze strony:
https://anydesk.com

Należy koniecznie przed rozpoczęciem szkolenia sprawdzić czy program AnyDesk pracuje prawidłowo z poziomu sieci uczestnika szkolenia. W przypadku wystąpienia problemów należy skontaktować się z prowadzącym szkolenie w celu uzyskania wsparcia technicznego zmierzającego do zaimplementowania konfiguracji zmierzającej do zapewnienia poprawnej pracy programu AnyDesk.

Stanowisko B

Komputer z systemem operacyjnym Windows oraz zainstalowanym oprogramowaniem klienckim VPN: **Stormshield IPSEC Client** oraz **OpenVPN**. Dostęp do pulpitu komputera jest realizowany przez program **AnyDesk**. Kod dostępu (ID) zostanie dostarczony przez organizatora szkolenia. Komputer stanowiska **B** posiada adres IP: 192.168.200.2. Komputer stanowiska **B** symuluje komputer użytkownika pracy zdalnej/ mobilnej.

Stanowisko C

Stanowisko **C** to dwa elementy: urządzenie **STORMSHIELD UTM** oraz **serwer usług**. W ramach warsztatów praktycznych uczestnik szkolenia będzie konfigurował urządzenie STORMSHIELD UTM w celu zapewnienia dostępu do usług na serwerze. Dostęp do urządzenia STORMSHIELD UTM jest możliwy bezpośrednio z poziomu komputera uczestnika (stanowisko A) po wcześniejszej autoryzacji. połączenia. Autoryzacji połączenia należy dokonać pod adresem: https://ssl.serwitech.com/auth - dane do poświadczenia zostaną dostarczone przez prowadzącego szkolenie (użytkownik/hasło).

Po autoryzacji urządzenie STORMSHIELD UTM stanie się osiągalne dla uczestnika szkolenia pod adresem: https://jmdi.serwitech.com:555/admin

Dane do logowania na UTM to: admin/admin. Urządzenie STORMSHIELD UTM ma adres zewnętrzny IP: 192.168.190.2.

Serwer usług ma adres IP: 172.16.10.2. Konfiguracja urządzenia STORMSHIELD UTM ma zapewnić dostęp do następujących zasobów na **serwerze usług** dla użytkowników mobilnych (zdalnych):

1. http://172.16.10.2 - port 80 poprzez metodę **SSL VPN PORTAL** (tunelowanie portów)
2. https://172.16.10.2 - port 443 poprzez metodę **PORT FORWARDING** (przekierowanie portów po wcześniejszej autoryzacji) - https://192.168.190.2:444
3. https://172.16.10.2:12320 - port 12320 poprzez metodę **OpenVPN**
4. https://172.16.10.2:12321 - port 12321 poprzez metodę **IPSEC VPN IKE v.2** (autentykacja za pomocą certyfikatów osobistych)

Uwagi

W czasie warsztatów skonfigurowane zostaną moduły/funkcjonalności urządzenia **STORMSHIELD UTM**:

- LDAP
- PKI
- Captive Portal
- SSL VPN Portal
- SSL VPN
- IPSEC VPN (mobile)
- Firewall
- NAT