## Vzpostavljanje VPN povezave

V razdelku je opisan postopek vzpostavitve povezave VPN z enkratnim geslom.

Uporabnik nima nameščenega odjemalca AnyConnect

1) Če uporabnik na delovni postaji nima nameščenega odjemalca VPN, v brskalniku najprej odpre povezavo <u>https://vpn.znet.si</u>.

2) Samodejno (in po potrebi z uporabnikovim dovoljenjem) se zažene funkcionalnost »Host Scan«, kar uporabnik v brskalniku vidi kot zagon »Cisco Secure Desktop«. Host Scan pri tem zajame podatke o nameščeni programski opremi na delovni postaji (anti virus, požarna pregrada).

Cisco	Secure Desktop
WebLaunch	Using Sun Java for Installation
<ul> <li>Platform Detection</li> <li>- ActiveX</li> <li>Java Detection</li> </ul>	Sun Java applet has started. This could take up to 60 seconds. Please wait
🗌 - Sun Java	
- WebLaunch - Access Denied	
- Critical Error - Success	Download
- Access Denied	

3) Uporabnik vpiše svoje uporabniško ime in geslo v ponujena polja. S tem se avtenticira.

Izberete ustrezen uporabniški profil in vpišete uporabniško ime v menijiski izbiri GROUP.

**zNET\_ZASEBNIK** – zasebni izvajalci zdravstvene dejavnosti **zNET** – vsi ostali uporabniki oddaljenega dostopa

3	Login
	Please enter your username and password.
	GROUP: ZNET  USERNAME:
	PASSWORD:
	Login

4) Namestitveni skript ugotovi, da odjemalec AnyConnect ni nameščen in ga namesti.

5) Ko je odjemalec nameščen, se zažene in vzpostavi virtualni omrežni vmesnik. Ker je uporabnik že avtenticiran, se povezava VPN vzpostavi brez ponovne avtentikacije.

## Uporabnik ima nameščenega odjemalca AnyConnect

1) Uporabnik zažene odjemalca AnyConnect s klikom na ustrezno ikono. Odpre se grafični vmesnik programa.



2) S klikom na »Connect« vzpostavi odjemalec povezavo z ASA na naslovu vpn.znet.si. Host Scan zajame podatke o nameščeni programski opremi na delovni postaji (anti virus, požarna pregrada).

3) Uporabnik vpiše uporabniško ime in PIN (geslo).

Group:	ZNET
Username:	smilanic@nil.si
Password:	I

4) ASA posreduje uporabniško ime strežniku RADIUS. Ta pošlje enkratno geslo na mobilno številko uporabnikovega telefona prek sporočila SMS.

5) Strežnik RADIUS odgovori požarni pregradi s sporočilom Challenge z ustreznim sporočilom. Uporabnik vpiše v polje »Answer« svoj PIN in geslo, ki ga je prejel prek SMS.

		_
Answer:		
Authentication I	Message	
ļ		-

6) Strežnik RADIUS preveri pravilnost uporabnikovih poverilnic. Če so te pravilne, odjemalec prikaže pozdravno sporočilo, kot mu ga posreduje ASA. Uporabnik ga sprejme/potrdi.

Dobi obobi v oni	ezju zNET!	*
OPOZORILO! Nepooblascen do	istop lahko sprozi kazenski pregon	r

7) Namestitveni skript preveri, ali je na delovni postaji nameščena starejša različica odjemalca, kot je na voljo na ASA. Če je na voljo novejša različica, se ta namesti.

8) Ko je odjemalec posodobljen (če je to potrebno), vzpostavi virtualni omrežni vmesnik in s tem povezavo VPN.

## Nastavitve in podatki o delovanju odjemalca

Ko je povezava VPN vzpostavljena, lahko uporabnik prek grafičnega vmesnika preveri prejete nastavitve in podatke o delovanju odjemalca. Te so na voljo prek različnih zavihkov grafičnega vmesnika, najvažnejši pa je »Statistics«.

sco Anycon	neer Secure woonity	Glient	
intual Private Networ	k (VPN)		
eferences Statistics Rout	a Details   Pirevail   Message History		
			1
Connection Information			
State:	Connected		
Tunnel Hode (IPv-K)	Tunnel All Traffic		
Tunnel Mode (IPv6):	Drop All Traffic		
Dunation:	00:07:47		
Address Information -			
Client (IPv4):	172.29.48.1		
Client (IPv6):	Not Available		
Serven	84.39.212.100		
Bytes			
Sent:	184220		
Received:	20303		
Frames			•
		1.0	

S slike so razvidni podatki o delovanju odjemalca. Ta je vzpostavil povezavo VPN (»Connected«). Ves promet z delovne postaje se »tunelira« in s tem šifrira (»Tunnel All Traffic«). Razvidni so:

- trajanje povezave,
- dodeljeni naslov odjemalca IPv4,
- javni naslov ASA, na katerem se zaključuje povezava VPN,
- količina prejetega in poslanega prometa IP,
- idr.