

### Preusmjeravanje porta kroz SSH tunel



Dok radimo na projektu koji testiramo na lokalnom računalu, pojavi se potreba da se napredak pokaže nekom od nadređenih, kolega s kojima surađujete ili nekome tko želi isprobati funkcionalost onoga što radite. Testiranje CMS Plone portala u mom slučaju zahtijevala je prijavu sa *AAI*@EduHr elektroničkim identitetom kojeg po pravilima prihvatljive upotrebe treba adekvatno zaštiti.

Pošto radimo na testnom sustavu koji je dostupan na adresi host.domena.hr:8080, nemamo preusmjeren promet na Apache port 80 kao na produkciji, ni sustav prijave koji se preusmjerava na https port 443 za kojeg je generiran odgovarajući Terena certifikat preko usluge Carneta. Autentikacijom na portu 443 enkripcijom prometa štitimo korisničke podatke.

Postavilo se pitanje kako zaštititi prijavu korisnika preko nezaštićenog porta 8080, a da pritom dodatno ne konfiguriramo Apache na portu 443, generiramo certifikat i sl. Jedno moguće rješenje je da se promet sa nezaštićenog porta 8080 preusmjeri kroz SSH tunel do koleginog računala.

Preusmjeravanje porta preko SSH konekcije omogućava da na točno određenom udaljenom računalu omogućimo siguran način prijave . Sav promet je enkriptiran između dva računala između kojih se promet odvija.

Kod testiranja CMS portala imamo situaciju da testna instanca radi na portu 8080 bez Apache servera, a želimo pristupiti s nekog vanjskog hosta.

Za svrhe testiranja posao su olakšale virtualne instalacije. Na dovoljno jakom stolnom računalu koje inače koristimo za sve druge poslove možemo stvoriti sasvim pristojan probni poligon i prebaciti na njega produkcijske stvari i nesmetano učiti na testnoj mašini umjesto na pravoj produkcijskoj koju bi neki testovi mogli privremeno onesposobiti.

Za potrebe postavljanja intraneta na postojeći CMS portal ustanove i povezivanje prijave preko na LDAP imenika ustanove napravljena je testna replika produkcije na Vbox-u. Debian Carnet instalacija je gostujuća na Debian Wheezy 64-bit desktopu.



### Preusmjeravanje porta kroz SSH tunel

Published on sys.portal (https://sysportal.carnet.hr)



Virtualni server za testiranje je u "bridge" modu i postavljen je na statičku IP adresu. Stranici koja se vrti na portu 8080 na siguran način možemo pristupiti kao u slijedećemo primjeru :

Kod kolege koji koristi Linux desktop pokrenemo naredbu u treminalu:

pingvin@desktop:~\$ ssh -R 8080:intra.simet.hr:8080 -C -N pingvin@desktop.simet.hr
pingvin@desktop.simet.hr's password:

Pri čemu je s lijeve strane port 8080 upućen klijentu, dok je s desne port 8080 koji prosijeđujemo. To može biti važno ako želimo promijenti proslijeđeni port u neki drugi, na primjer 8081. Pri tome -R specificira da će port na udaljenom računalu biti preusmjeren na lokalni port na klijentskoj strani, a konekcija ide sigurnim kanalom. Port 8080 sa udaljenog računala se prosljeđuje na port 8080 na klijentskoj strani. Opcija -C zahtijeva kompresiju svih podataka koji prolaze kroz SSH tunel, dok -N sprečava pokretanje naredbe na udaljenom računalu

Poslije unosa ispravne lozinke bez zatvaranja terminala unesemo u internet preglednik localhost:8080/simet/login\_form otvara se forma za prijavu koju smo zaštitili SSH tunelom.



🔹 🔞 localhost:8080/simet/login_form	s <b>4</b> 8 € 2 ÷ 8
STEALURSKI FAKULTET	
Početak Nastava Zranost Oltakulletu Dokumenti Poveznice Katalog informacija	Osiguravanje kvalitete Alumni English
Vi sie ovdje: Početak	
	Login Name
	Zaporka
	Prijava
Zaboravili ste zaporiku? If you have forgotion your password, we can send you a new one.	
	(c)/2009,Sveudiliste u Zagrebu,Metalurški fakultet
	Powered by Plone & Python

Radi potrebe da se demonstrira rad sa portalom za veći broj ljudi istovremeno s Windows klijenta, trebalo je istu stvar napraviti za Windows okruženje. Za to smo iskoristili svim sistemcima poznati PuTTY besplatni telnet-ssh klijent za Windows.

Jednostavno pokrenemo PuTTY na koleginom Windows 7 računalu, unesemo podatke za ssh konekciju prema hostu i spremimo session pod imenom "intra".



🕵 PuTTY Configuration		×	
Category:			
	Basic options for your PuTTY session		
Logging	Specify the destination you want to conn	ect to	
⊡ · Ieminal	Host <u>N</u> ame (or IP address)	<u>P</u> ort	
Bell	intra.simet.hr	22	
Features     Features     Window     Appearance     Behaviour     Translation     Selection     Colours     Connection     Proxy     Telnet     Rlogin     SSH     SSH     Serial	Connection type:		
	Load, save or delete a stored session Sav <u>e</u> d Sessions intra Default Settings intra	Load Save	
	Close window on e <u>xi</u> t:	clean exit	
About	 Open	<u>C</u> ancel	

Pod opcijom "Tunnels" uredimo opcije kao na slijedećem primjeru.



# **Preusmjeravanje porta kroz SSH tunel** Published on sys.portal (https://sysportal.carnet.hr)

🕵 PuTTY Configuration	n			×
Category:				
Terminal		Option	s controlling SSH po	ort forwarding
Keyboard		Port forwarding		
Features		Local ports a	accept connections	from other hosts
- Window		Remote port	s do the same (SSH	I-2 only)
Appearance		Forwarded ports	S:	Remove
Behaviour				
Iranslation				
Colours				
		Add new forwar	rded port:	
Data	Ξ	Source port	8080	Add
Proxy Tolget		Destination	localhost:8080	
		Local	Remote	Dynamic
⊡- SSH		Auto	◎ IPv4	◎ IPv6
Kex				
i Auth				
×11				
Tunnels				
Bugs	Ŧ			
About			Open	Cancel

Dodamo u proslijeđene portove sa "Add".



🕵 PuTTY Configuratio	n			×
Category:				
- Teminal		Options	controlling SSH po	rt forwarding
Keyboard		Port forwarding		
Features		Local ports a	ccept connections	from other hosts
⊡. Window		Remote ports	s do the same (SSH	l-2 only)
Appearance		Forwarded ports	c .	Remove
Behaviour		L8080 local	host:8080	
Colours				
		Add new forward	ded port:	
Data	=	Source port	8080	Add
···· Proxy		Destination	localhost:8080	
Riogin		Local	Remote	O Dynamic
SSH		Auto	IPv4	© IPv6
Kex				
-X11				
···· Tunnels				
Bugs	Ŧ			
About			Open	Cancel

Pokrenemo "Open" nakon kojeg dobivamo uobičajeno pitanje o ključevima koje pronalazimo sa "Yes"



## Preusmjeravanje porta kroz SSH tunel





Poslije sve izgleda kao klasično spajanje sa SSH.



Ako smo sve uspješno napravili, vidjet ćemo upozorenje "Windows firewalla" da se nešto preko ssh pokrenulo i traži vaše dopuštenje za pristup računalu, što u ovom slučaju dopuštamo.



Indows Security Alert				
💮 Windo	ws Firewal	l has blocked some features of this program		
Windows Firewall h private networks.	as blocked some	e features of SSH, Telnet and Rlogin client on all public and		
	<u>N</u> ame:	SSH, Telnet and Rlogin dient		
	Publisher:	Simon Tatham		
	Pat <u>h</u> :	C:\users\korisnik\downloads\putty.exe		
Allow SSH, Telnet a	and Rlogin client	to communicate on these networks:		
Private netw	orks, such as m	y home or work network		
<b></b> P <u>u</u> blic netwo because the	rks, such as the se networks off	ose in airports and coffee shops (not recommended ten have little or no security)		
What are the risks	of allowing a pr	ogram through a firewall?		
		Allow access Cancel		

Kad smo propustili ovu konekciju kroz Windows firewall, pokrenemo web preglednik, pozovemo adresu koju smo zadali kao ciljanu ("localhost:8080") i pristupimo našoj tuneliranoj stranici testnog virtualnog servera te se dalje preko web stranice prijavimo sa elektroničkim identitetom na portal.





Time osiguravamo da AAI@EduHR podaci ne prolaze mrežom u čitljivom obliku. Ali kolege će sigurno pronaći i drugačije primjene za ovakvo spajanje, na primjer u slučajevima da treba proći kroz blokadu postavljenu na vatrozidu.

sri, 2014-04-09 13:56 - Goran Šljivić**Vijesti:** <u>Linux</u> [1] **Vote:** 0

No votes yet

**Source URL:** https://sysportal.carnet.hr/node/1373

#### Links

[1] https://sysportal.carnet.hr/taxonomy/term/11