# EXCHANGE 2010 – VODIČ ZA OUTLOOK ANYWHERE
**verzija 1.1**

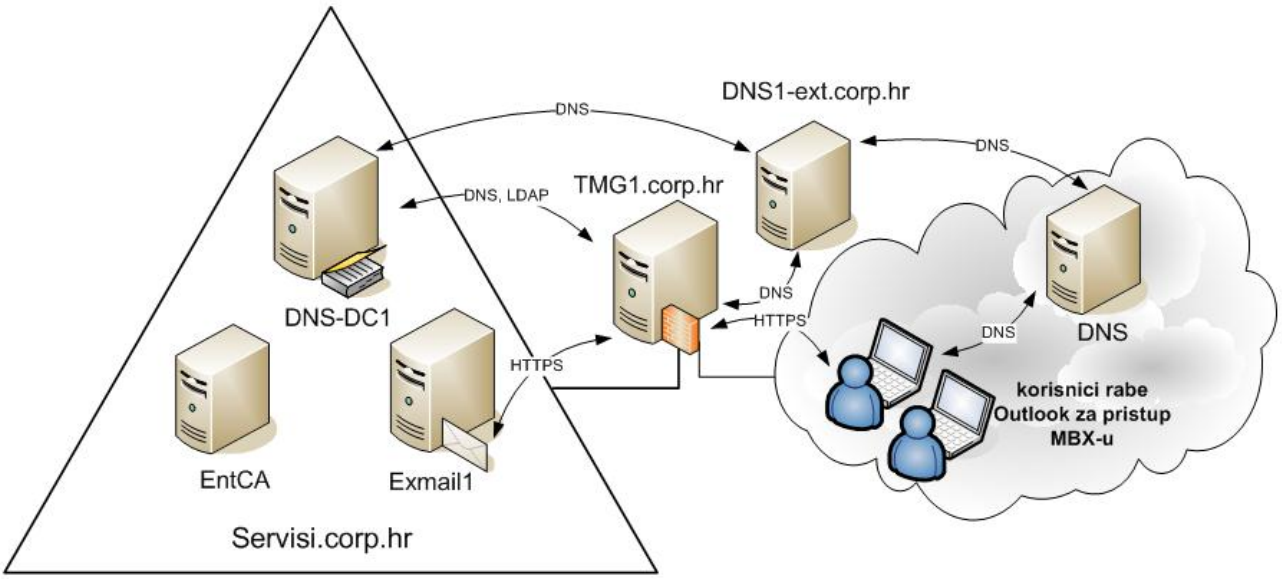
## 1. UVOD

Namjena je ovog članka olakšati sistemcima uspostavu Outlook Anywhere funkcionalnosti u sustavu e-pošte središte kojega je Exchange 2010 a periferija Outlook 2007/2010. Tema je slojevita a ovo je ipak samo članak, stoga ćemo svjesno ignorirati sve što nije u najdirektnoj sprezi sa postavljanjem Outlook Anywhere tipa komunikacije. Rečeno ujedno implicira i dostatnu razinu upućenosti čitatelja u Exchange problematiku. Prije nego što se ozbiljnije pozabavite s Outlook Anywhere, svakako Outlookom i Internet Explorerom napadnite taj isti Exchange s LAN-a, rabeći pri tome iste korisničke accounte, pa i računala, koje planirate iskoristiti za testiranje rada Outlook Anywhere.

## 2. PREGLED INFTRASTRUKTURNIH KOMPONENATA

Da bi sve skupa bilo razumljivo i, naposljetku, upotrebljivo (što je svrha postojanja ovog teksta), infrastruktura sustava je uprošćena tj. namjerno su izbačene razne komponente koje osiguravaju visoku razinu postojanosti, dostupnosti i zaštite sustava kao cjeline. Dakle, kako je vizualizirano slikom 1, naš Exchange sustav, kojemu ćemo pristupati rabeći Outlook Anywhere funkcionalnost, ima ove gradive dijelove:

- operativni sustav na svim serverima je Windows 2008 R2; serveri mogu biti fizički ili virtualni
- forest servisi.corp.hr je jednodomenski, u Windows 2008 R2 režimu rada; drži ga Domain Controller dns-dc1.servisi.corp.hr;
- dns-dc1.servisi.corp.hr je ujedno interni DNS; nadležan je i za interni resolving hostova DNS domene **corp.hr**; u DMZ segmentu je dns1-ext.corp.hr, autoritativan za vanjski resloving hostova DNS domene corp.hr; jasno, vanjski DNS je postavljen kao forwarder internom DNS-u;
- exmail1.servisi.corp.hr – nadležan je za SMTP domene servisi.corp.hr i **corp.hr**; obnaša sve Exchange uloge osim Unified Messaging;
- entca.servisi.corp.hr je Enterprise Certification Authority; obnaša uloge *root* i *issuing* CA;
- tmg1.corp.hr je *stand-alone* Threat Management Gateway 2010, smješten je u DMZ; jednom nožicom komunicira s Internet a drugom s LAN resursima; kroz njega Outlook klijenti s Interneta pristupaju Exchange funkcionalnostima.




**Slika 1**: Vizualizacija komponenata sustava.

Važno je uočiti postojanje SMTP/DNS domene **corp.hr** te razumjeti implikacije toga. Očito je naša firma na Internetu predstavljena domenskim sufiksom corp.hr, i s tom činjenicom na umu mi moramo konfigurirati:

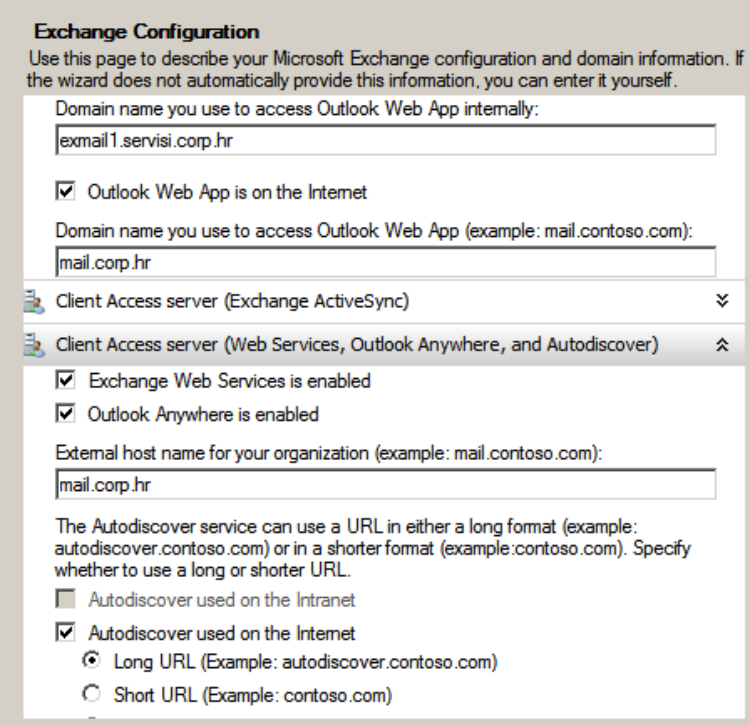
- interni i eksterni DNS;
- Exchange organizaciju glede SMTP domena za koje je nadležna, internih i eksternih URL-ova, sufiksa korisnikove SMTP adrese te certifikat za Exchange server;
- Web Listener i Firewall Policy na TMG sloju;
- Outlook klijente.

Glede DNS-ova, u domenu corp.hr upišemo odgovarajuće A i MX zapise. Za potrebe ovog vodiča Internet ime usluge e-pošte je **mail.corp.hr**. Samo vodite računa da se na vanjskom DNS-u IP vrijednost A zapisa odnosi na IP adresu vanjske nožice TMG-a.

Obrada ostalih koraka slijedi.

## 3. CERTIFIKATI ZA SERVISE I RAČUNALA

Outlook Anywhere odbija raditi s Exchangeovim *self-signed* certifikatom. Ako je domenski CA ispravno podešen, nije teško dobiti od njega serverski certifikat i to na onaj elegantniji način, rabeći EMC: ogranak Server Configuration > naredba New Exchange Certificate. Kako bismo izbjegli probleme s XP Professional i/ili ranijim verzijama Outlooka kad rabe Outlook Anywhere, tijekom procedure kreiranja certifikata kao **Common Name** postavit ćemo ime **mail.corp.hr**; tada druga imena – za Outlook Anywhere je važno i autodiscover.corp.hr - idu u Subject Alternative Name. Upravo to ćemo postići ako tijekom izrade zahtjeva za certifikatom radimo kao na slici 2.




**Slika 2**: Tijekom procedure New Exchange Certificate definiramo imena Exchange servisa.

New Exchange Certificate završava kreiranjem datoteke tipa .req. Odmah ju otvorimo Notepadom, ostavimo tako, potom se prebacimo na Internet Explorer kojime pristupimo Web enrollment adresi EntCA poslužitelja - u našem slučaju to bi bilo https://entca/certsrv - i tu slijedimo smjer Request a certificate > Advanced certificate request > Submit a certificate request by using a base-64 encoded.... Ovdje, u polje Saved Request, ukopiramo kompletan sadržaj .req datoteke. Nakon toga preostaje skidanje certifikata, ali **pazite** da prethodno uključite opciju Base 64 encoded.

Vratimo se u EMC, označimo aktualni zahtjev i biramo naredbu Complete Pending Request. Naposljetku još trebamo primijeniti certifikat na Exchange servise, što postižemo naredbom Assign Services to Certificate.

Predmetni certifikat moramo primijeniti i na tmg1.corp.hr server. Stoga ćemo na Exchange serveru iskoristiti snap-in Certificates kako bismo izvezli certifikat zajedno s privatnim ključem i uključenom opcijom Include all certificates... u .pfx (PKCS #12) format; potom ćemo na tmg1.corp.hr, njegovim Certificates snap-inom, uvesti taj certifikat u mapu Personal računala (ne korisnika).

**Ne zaboravite** da u Trusted Root Certification Authorities Exchange i TMG servera, te Outlook računala, morate smjestiti, ručno ili autoenrollmentom, certifikat PKI servisa podignutog na entca.servisi.corp.hr.

## 4. KONFIGURIRANJE EXCHANGEA

Pretpostavljamo ispravan rad Exchange poslužitelja na LAN-u.

- Prije uključivanja Outlook Anywhere obilježja, uvjeriti se da je djelatano obilježje (feature) RPC over HTTP Proxy;
- uključiti Outlook Anywhere: EMC > Server Configuration > Client Access > desni klik na serveru > Enable Outlook Anywhere;
- podesiti Outlook Anywhere: desni klik na serveru > Properties > kartica Outlook Anywhere i ovdje u polje External host name upisati izraz mail.corp.hr, također uključiti Basic authentication;
- upisati mail.corp.hr kao osnovu externih URL-ova za ECP, OAB i OWA: EMC > Server Configuration > Client Access > kartice u srednjem oknu;
- IIS Manager > Default Web Site > RPC > Authentication > uvjeriti se da je uključena Basic autentikacija te u polje Default domain upisati FQDN domene u kojoj je Exchange - servisi.corp.hr.

## 5. KONFIGURIRANJE TMG-a

Podrazumijevamo da je TMG ispravno konfiguriran za obnašanje uloge tzv. Edge firewalla i routera, te da je njegovoj vanjskoj nožici dodijeljena Internet IP adresa hosta mail.corp.hr (to je situacija kojom je najlakše ovladati). Preostaje nam kreiranje Web listenera i Firewall direktive za Outlook Anywhere.

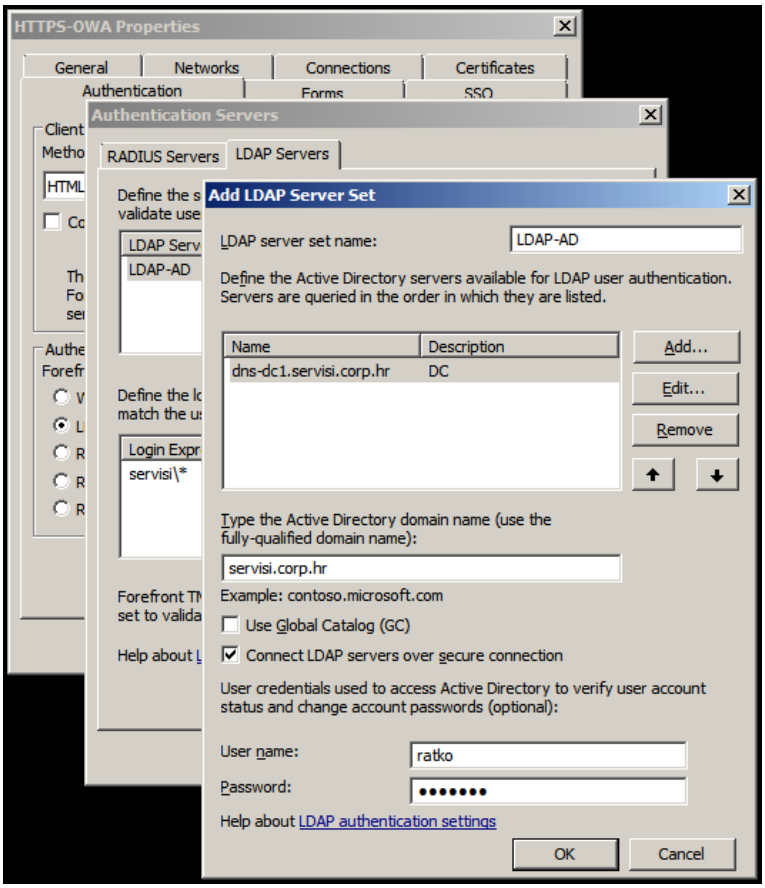
### Web Listener

U Forefront TMG konzoli smještamo se na ogranak Firewall Policy, potom: kartica Toolbox > desni klik na mapi Web Listener > čarobnjak New Web Listener. Tijekom procedure kreiranja Web listenera poštivati niže instrukcije – opcije razmještene po karticama Web listenera - mada nije strašno i ako fulamo jer se svaki jednom kreirani Web listener kasnije može temeljito preinačiti.

- kartica **Networks**: uključiti samo mrežu External, u našem slučaju to treba biti IP adresa TGM-ovog mrežnog sučelja za vanjsku mrežu
- kartica **Connections**: uključiti obje opcije u okviru Client Connection Type i opciju Redirect all trafic from HTTP to HTTPS
- kartica **Certificates**: odabrati opciju Assign a certificate for each IP address; pod gumbom Select Certificate ne samo odabrati nego i provjeriti kako TMG prihvaća certifikat
- kartica **Authentication** (vidi sliku 3):
  - Client Authentication Method je HTML Form Authentication; Authentication Validation Method je LDAP (Active Directory)
  - pod gumbom Configure Validation Servers treba se nalaziti barem jedan LDAP Server Set s barem jednim Domain Controllerom (dobro je da taj bude i Global Catalog)
  - Login expression: servisi*

- pod gumbom Advanced uključiti opciju Require all users to authenticate a u polje Domain name upisati logon Windows domenu u NetBIOS obliku
- primijenite i parametre s kartice u fokusu slike 3

- kartice **Forms** i **SSO** su nebitne u ovom scenariju.




**Slika 3**:
Kartica Authentication Web listenera ima 3 razine, u fokusu je najniža razina.

**Firewall Policy**

U Forefront TMG konzoli smještamo se na ogranak Firewall Policy, fokusiramo potom karticu Tasks i, naposljetku, pokrećemo čarobnjak Publish Exchange Web Client Access. Najvažnije je odmah odabrati Exchange 2010 kao verziju Exchangea i uključiti opciju za Outlook Anywhere. Nakon toga, tijekom procedure kreiranja FW direktive, poštujte niži pregled direktive po karticama. Svaki eventualni propust lako se otkloni nakon kreiranja direktive.

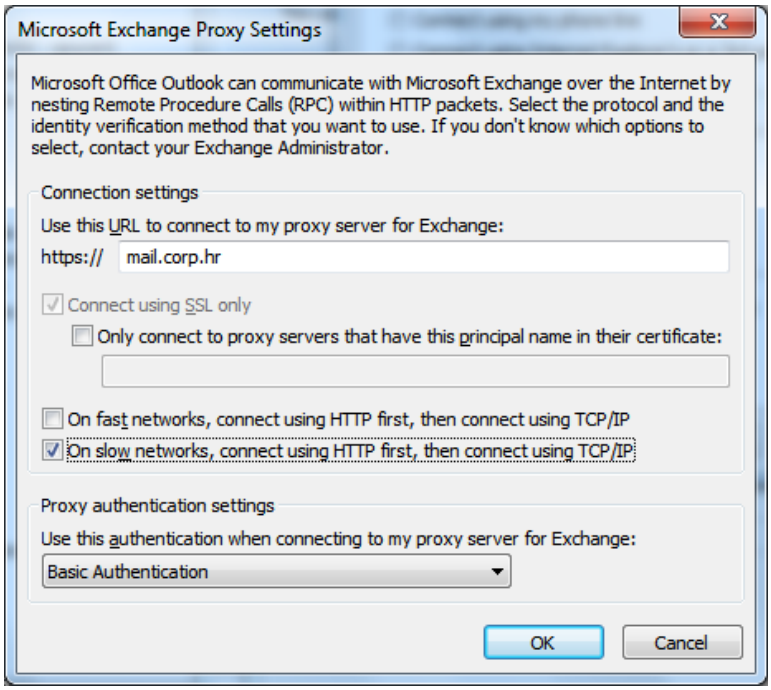
kartica **General**: opcija Enable mora biti uključena
kartica **Action**: opcija Allow mora biti uključena
kartica **From**: Anywhere
kartica **To**: u prvom polju treba biti interno FQDN Exchange servera, dakle, exmail1.servisi.corp.hr; u drugom polju njegova IP adresa; uključiti opcije Forward the original host header.... i Requests appear to come from the Forefront TMG computer
kartica **Traffic**: sadrži protokole HTTP i HTTPS
kartica **Listener**: sadrži referencu na Listener kojega smo kreirali u prethodnom koraku
kartica **Public Name**: odabrati Requests for the following Web sites, upisati mail.corp.hr
kartica **Paths**: mora sadržavati izraz *<same as internal> /rpc/**
kartica **Authentication Delegation**: uključiti Basic authentication
kartica **Application Settings**: opcija Use customized HTML forms... mora biti isključena
kartica **Bridging**: uključiti opciju Web server i Redirect requests to SSL port 443
kartica **Users**: All Authenticated Users
kartica **Schedule**: odabrati Always
kartica **Link Translation**: uključiti Apply link translation to this rule

Gornji se opisi Web listenera i FW direktive odnose na naše potrebe i polučit će očekivani rezultat u situaciji opisanoj pod naslovom Pregled infrastrukturnih komponenata.

## 6. KONFIGURIRANJE OUTLOOK KLIJENTA

Računamo s time da je Office 2007/2010 uredno instaliran na Windows 7 te da se ranije niste previše zaigrali s raznim opcijama Outlooka. Inicijalnu konfiguraciju Outlooka tj. otvaranje računa odradite na LAN-u, provjerite rad... i tada krećemo s prilagodbom za Outlook Anywhere:

- u Trusted Root Certification Authorities računala importirati certifikat CA koji je Exchangeu izdao certifikat;
- Account Settings > kartica E-mail > gumb Change > gumb More Settings > kartica Connection i tu uključiti opciju Connect to MS Exchange using HTTP;
- u kartici Connection, pod gumbom Exchange Proxy Settings, u polje https:// upisati mail.corp.hr; uključiti opciju On slow networks...; odabrati Basic Authentication (opcija Using SSL only mora biti uključena ali u polju ispod ništa);
- restartati Outlook.




**Slika 4**: Outlook je podešen za aktualni scenarij.

Kad tako podešeno računalo spojimo na Internet, dobit će mrežne parametre od ISP-a – IP adresu i DNS-ove. Pokretanjem Outlooka započinje pretraga DNS hijerarhije za IP adresom hosta mail.corp.hr. Budući da je naš dns1-ext.corp.hr pristupačan s Interneta, zapis mail.corp.hr bit će resolviran u IP adresu vanjske nožice TMG-a, na kojoj sluša Web listener, na portu TCP 443. HTTPS-om mi napadamo baš taj port. TMG će zatražiti autentikaciju, ulogirajte se rabeći format domena\korisnik i... – JUPIII – Outlook komunicira s TMG-om, ovaj s Exchangeom... i sve 5!

Završna napomena: Kako je već rečeno, odabran je pojednostavljen scenarij, znači, zanemarene su neke mogućnosti & opcije koje se u realnim situacijama možda neće smjeti ignorirati. U svakom slučaju, kad jednom stvorimo funkcionalan sustav, lako ga je nadalje dotjerivati i prilagođavati.

Ratko Žižek

*< kraj >*