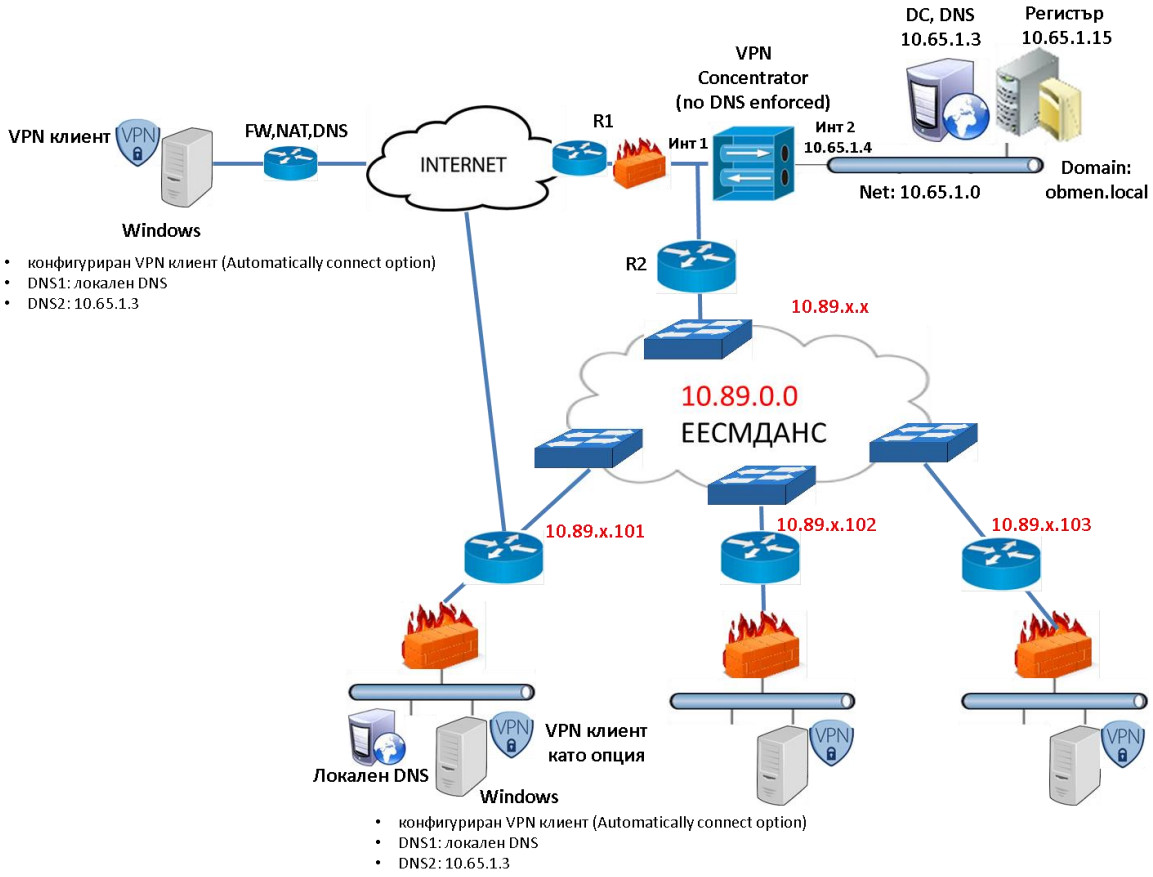
Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
ДЪРЖАВНА АГЕНЦИЯ „ЕЛЕКТРОННО УПРАВЛЕНИЕ“

СИСТЕМА ЗА ЕЛЕКТРОНЕН ОБМЕН НА СЪОБЩЕНИЯ (СЕОС)

МРЕЖОВА СВЪРЗАНОСТ



Фиг1. Принципна схема на мрежова свързаност

За осигуряване на мрежова свързаност се използва транспортната среда на ЕЕСМДАНС, както и връзки през Internet.

Централен сайт

Централният сайт е оборудван с необходимите мрежови устройства (маршрутизатори, защитна стена, комутатори и VPN концентратор), които осигуряват свързаността му към ЕЕСМДАНС, към Internet и към вътрешен LAN сегмент (10.65.1.0). Във вътрешния LAN сегмент са инсталирани и адресирани Domain Controller, DNS сървър и сървър с регистри. Създаден е вътрешен домейн **obmen.local**. Във VPN концентратора е дефиниран VPN адресен пул (IP мрежа клас А – 10.65.0.0) за потребителите. В Domain контролера за всеки участник е създаден

потребителски акаунт с атрибути за достъп (user name, password), на който е присвоен статичен IP адрес от този пул.

I. Свързаност на участниците през Internet

Транспортната Internet среда осигурява достъп до граничен маршрутизатор R1 на централния сайт. Маршрутизатор R1 притежава интерфейс с публичен IP адрес и същевременно е свързан към интерфейс 1 на VPN концентратора. Локалния сървър на участника изгражда Remote Access VPN връзка през Интернет към VPN концентратора, при което на сървъра автоматично се присвоява статичен VPN IP адрес от зададения пул (например 10.65.1.100). Свързаността през VPN осигурява DNS услуга за домейн obmen.local, достъп до сървъра с регистри и достъп до сървърите на всички останали участници.

II. Свързаност на участниците през ЕЕСМДАНС

2.1. Транспортната среда

В инфраструктурата на ЕЕСМДАНС е конфигуриран отделен VLAN (VLAN-Z). Маршрутизатор R2 притежава интерфейс с IP адрес от VLAN-Z и същевременно е свързан към интерфейс 1 на VPN концентратора. Адресирането във VLAN-Z се извършва съгласно IP схема, предоставена от ДАЕУ. Организации, които са свързани в тази среда имат достъп до граничния маршрутизатор R2 на централния сайт, като използват собствени маршрутизатори. За целта в тях се конфигурира физически или виртуален интерфейс, свързан към VLAN-Z на комутатора за достъп към ЕЕСМДАНС. Устройствата на организациите осигуряват свързаност от вътрешния LAN сегмент на локалния сървър до IP мрежа 10.89.0.0 и в частност до маршрутизатор 2.

2.2. Достъп чрез Remote Access VPN през ЕЕСМДАНС

Локалния сървър на участника изгражда Remote Access VPN връзка през ЕЕСМДАНС към VPN концентратора, при което на сървъра автоматично се присвоява статичен VPN IP адрес от зададения пул (например 10.65.3.100). Свързаността през VPN осигурява DNS услуга за домейн obmen.local, достъп до сървъра с регистри и достъп до сървърите на всички останали участници.

ДОПУСКАНИЯ И ОГРАНИЧЕНИЯ

1. За VPN концентратор се изпълнява Windows Server с конфигурирана роля Routing And Remote Access Server (RRAS), Cisco ASA 55xx или други еквивалентни устройства, способни да терминират VPN връзки, инициирани от стандартен Windows VPN client.
2. Локалните сървъри на участниците са с Windows операционни системи и използват стандартен Windows VPN клиент.
3. За автоматизиране на процесите се използва вградената функционалност Task Schedule на Windows. Това позволява след първоначалното конфигуриране на VPN клиента, VPN връзката автоматично да се активира със стартирането на операционната система, по зададен интервал автоматично да проверява за свързаност и да не се прекъсва при прекратяване на локалната сесия (Log Off) на потребител.
4. Организациите, използващи ЕЕСМДАНС разполагат с локални маршрутизатори и необходимото мрежово оборудване.
5. Осигуряването на необходимата IP свързаност към VLAN-Z може да изисква допълнителни настройки в съществуващи устройства (например защитна стена), които вече са конфигурирани в NAT за целия LAN сегмент на организацията, както и разрешаване на протоколи PPTP и GRE. Крайната цел е локалния сървър да има мрежова свързаност до маршрутизатор 2 във VLAN-Z.
6. В случай, че е необходимо локалния сървър да използва и друга DNS услуга (например за вътрешен домейн на организацията) е необходимо корекция в DNS настройките на този сървър.

7. ДАЕУ ще предостави IP план за адресиране и конфигуриране на мрежоеите устрйства във VLAN-Z и ще изготви подробни инструкции за настройка на VPN клиент на локалните сървъри за операционни системи Windows 7, Windows Server 2003, 2008, 2012 и Linux.

8. Участниците са потвърдили, че не използват (и няма да използват) IP мрежа 10.65.0.0/16 за други цели в локалната си IP адресация.

9. За изпълнение на схемата за свързаност ДАЕУ осигурява необходимите компонени за централния сайт, но не се ангажира с осигуряването на хардуер или софтуер за участниците.