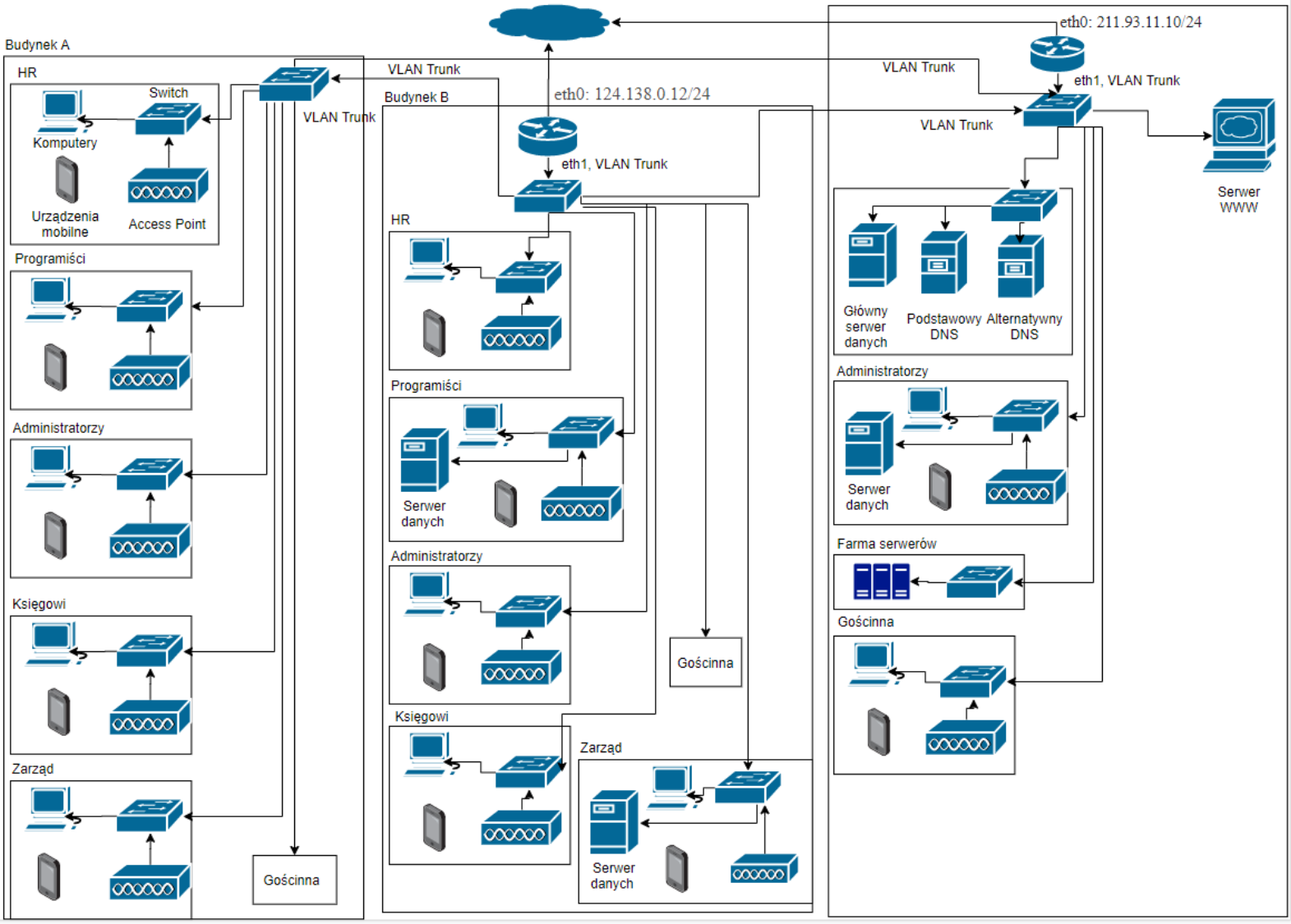
Damian Werpachowski

1. Schemat sieci



Na wstępie przepraszam za te groty na końcach strzałek, ich oczywiście być nie powinno, ale nie wiedziałem jak ich się pozbyć w narzędziu, z którego korzystałem. W budynku B i C znajduje się po jednym routerze. W budynkach A, B, C znajduje się po jednym głównym switchu, wszystkie połączone VLAN Trunkiem, każdy z każdym. Routery łączą się po interfejsach eth0 z Internetem oraz po eth1 z głównymi switchami (VLAN Trunk) w swoich budynkach. Każdy dział posiada switch, połączony z głównym switchem w swoim budynku; access point dla połączeń bezprzewodowych; komputery. Każdy dział stanowi osobną sieć VLAN. Dział programistyczny, administratorzy i zarząd posiadają osobne serwery danych - w pierwszym przypadku ze względu na wygodę i potencjal-

nie wyższe zapotrzebowanie, w drugim ze względów bezpieczeństwa. Dział HR i księgowy do przechowywania własnych danych używa głównego serwera danych. Wymiana danych między działami odbywać się może za pomocą głównego serwera danych.

Nazwa	VLAN
Routery	VLAN 1
Serwer WWW	VLAN 2
DNS i dane	VLAN 3
Gościnna	VLAN 4
Farma serwerów	VLAN 5
Zarząd	VLAN 6
HR	VLAN 7
Programiści	VLAN 8
Administratorzy	VLAN 9
Księgowi	VLAN 10

2. Ilość urządzeń

- 2 routery
- 18 switchy
- 14 access pointów
- 4 serwery danych
- 2 serwery DNS
- 1 serwer WWW

3. Tablice tras

Niech interfejsy eth1 routerów B i C mają adresy IP odpowiednio 10.1.0.1 oraz 10.1.0.2. Routery będą zapewniać m.in. Inter-VLAN routing.

Router w budynku B

cel	brama	maska	interfejs
0.0.0.0	124.138.0.23	0.0.0.0	eth0
10.2.0.0	0.0.0.0	255.255.0.0	eth1/2
10.3.0.0	0.0.0.0	255.255.0.0	eth1/3
10.4.0.0	0.0.0.0	255.255.0.0	eth1/4
10.5.0.0	0.0.0.0	255.255.0.0	eth1/5
10.6.0.0	0.0.0.0	255.255.0.0	eth1/6
10.7.0.0	0.0.0.0	255.255.0.0	eth1/7
10.8.0.0	0.0.0.0	255.255.0.0	eth1/8
10.9.0.0	0.0.0.0	255.255.0.0	eth1/9
10.10.0.0	0.0.0.0	255.255.0.0	eth1/10

W przypadku routera w budynku C zmienia się jedynie brama w pierwszym wierszu na 211.93.11.224.

Gdy połączenie routera B z Internetem ulegnie awarii, należy zmienić jego pierwszy wpis na:

cel	brama	maska	interfejs
0.0.0.0	10.1.0.2	0.0.0.0	eth1/1

Czyli należy przekierowywać cały ruch kierowany do Internetu, na interfejs eth1, na VLAN 1, tak, by dotarł do routera w budynku C.

Gdy połączenie routera C z Internetem ulegnie awarii, należy uczynić analogiczną modyfikację, tylko że jako bramę należy ustawić 10.1.0.1, czyli adres routera B.

4. Reguły NAT

Fiewall i NAT na routerze w budynku C są tak skonfigurowane, by ruch przychodzący na porty 80 i 443 na adres 211.93.11.10/24 (adres routera) był kierowany do serwera WWW. Poza tym, fiewall konfigurujemy na obu routerach tak, by blokować ruch przychodzący, inicjowany z zewnątrz.

Fiewall blokuje ruch z sieci gościnnej do reszty firmy. Ponadto powinien być blokowany ruch z serwera WWW do reszty firmy, tak, by serwer WWW nie mógł zostać wykorzystany do uzyskania dostępu do wnętrza firmy.

5. DHCP

Oba routery są wyposażone w DHCP. N-ty VLAN dostaje pulę adresów 10.N.0.0/24. Aby serwery DHCP nie przydzieliły tych samych adresów dwóm różnym hostom, ustalmy, że router B będzie N-temu VLANowi przydzielać adresy z pierwszej połowy puli 10.N.0.0/24, natomiast router C z drugiej połowy. Można zarezerwować adresy (na przykład przydzielić statycznie) routerów (konkretnie interfejsów eth1), serwerów danych, WWW i DNS, aby się nie zmieniały. DNS i DHCP mogą współpracować by zapewnić nazwy domenowe dla hostów, typu dział123.internal.datavac.pl.

6. DNS

Firma posiada podstawowy i alternatywny serwer DNS. Ich celem jest cacheowanie odwzorowań domenowych oraz zapewnienie odwzorowań nazw hostów na ich adresy IP, na użytek wewnętrzny firmy. Strona WWW firmy posiada domenę zarejestrowaną u zewnętrznego dostawcy DNS. Domena odwzorowywana jest na adres 211.93.11.10, tj. router w budynku C. Sieć gościnna przy połączeniu z Internetem używa usług DNS firmy Google.

7. Wymagania ogólne

1. Należy zapewnić bezpieczny transfer i swobodne współdzielenie danych w obrębie poszczególnych działów.

Działy HR i Księgowy trzymają swoje dane w głównym serwerze danych, natomiast Programistyczny, Administracyjny i Zarząd mają własne serwery danych.

2. Należy zapewnić szczególną ochronę podsieci działu zarządu.

Zarząd znajduje się w VLAN 6. Posiada własny serwer danych. Zabezpieczenia w warstwie aplikacji takie jak logowanie.

3. W każdym budynku należy zapewnić dostęp do Internetu także dla gości firmy (w taki sposób, aby goście nie mieli dostępu do zasobów firmowych).

W każdym budynku znajduje się sieć gościnna (VLAN 4). Udostępnia komputery stacjonarne dla gości oraz sieć Wi-Fi. Nie posiada dostępu do reszty firmy - pakiety dostaną się do routera, gdzie, jeśli nie będą kierowane do internetu, to zostaną odrzucone. Korzysta z usług DNS firmy Google.

4. W każdym budynku powinna być zainstalowana sieć przewodowa zbudowana na bazie Ethernetu i sieć bezprzewodowa zbudowana na bazie Wi-Fi.

Każdy dział posiada switch oraz access point dla Wi-Fi.

5. Każdy z działów powinien mieć możliwość udostępniania danych wyłącznie pracownikom swojego działu (dla innych działów te dane nie powinny być dostępne).

Tak jak wspomniałem w punkcie 7.1, działy mają dostęp do serwerów danych. Ograniczenie by dane były niewidoczne dla innych działów zapewnia się w warstwie aplikacji, np. poprzez logowanie.

6. Powinna być także możliwość udostępniania pewnych danych wszystkim pracownikom firmy w taki sposób, by nie były one dostępne bezpośrednio z sieci zewnętrznej.

Służy do tego główny serwer danych.

7. Firma będzie chciała udostępniać własny serwis WWW.

Firma posiada serwer WWW obsługujący stronę www.datavac.pl. Usługę DNS zapewnia zewnętrzny dostawca. Strona jest dostępna pod adresem IP 211.93.11.10 (adres routera C), skąd jest kierowana do serwera WWW wewnątrz firmy.

8. Poszczególne działy firmy potrzebują serwerów z różnego rodzaju oprogramowaniem: systemem zarządzania projektami, bazą danych, repozytorium.

Zapewniają to wyżej wspominane serwery danych.