3.dia

GERGŐ kezd Sopronnal

A soproni telephelyen van a cég raktára.

Itt üzemel a Linux szerver, ami biztosítja a belső intranetes oldal elérését,

szolgáltatások:

* DNS
* Apache webszerver
* SSH
* FTP
* Samba - fájlszerver

A hálózatban 3 vlan található, 2 db 3650-24ps multilayer switch, 2 db 2960-24tt switch, 3 db 2911 router, 1 db wrt 300n wireless router, 6 db pc, és 2 db laptop.

Tartalmaz etherchannel megoldást, illetve a wirelessrouter dhcp-n keresztül osztja a címeket. A többi eszköz statikus ip címet kapott az egyszerűbb hibamenedzselés miatt.

5.dia

Hálózati logikai struktúrája

A hálózat logikai struktúrája arra utal, hogy hogyan van kezelve, szervezve és irányítva az adatforgalom a hálózaton belül. Ez a struktúra kulcsfontosságú az adatáramlás és a hálózati teljesítmény biztosítása érdekében. A Szálkapari Zrt.-nél a hálózat különböző alhálózatokra és VLAN-okra (Virtual Local Area Networks) van osztva a biztonság növelése, a forgalom hatékony kezelése és a teljesítmény javítása érdekében.

Minden helyszínen, például a győri központban, a soproni raktárban és a pozsonyi üzletben, a disztribúciós réteg több logikai részre van osztva. Ez az osztás VLAN-ok segítségével történik, amelyek az eltérő típusú hálózati forgalom szétválasztását szolgálják. Például a raktárban lehetnek VLAN-ok az árukezelés, a logisztika és az adminisztratív feladatok számára..

Sopron 3 db

Győr 5 db

Pozsony 4 db

7.dia

A VPN (Virtual Private Network) konfigurációja és implementációja alapvető fontosságú a két szervezet belső hálózatai közötti biztonságos kommunikációhoz.

A soproni szerver és a pozsonyi szerver kommunkációját VPN kapcsolattal valósítottuk meg.

A hálózat dinamikus forgalomkezelését az OSPF (Open Shortest Path First) protokoll segítségével oldják meg. A telephelyenként van egy határ router, ami elosztási pont (gerinc) az **Area 0**-hoz tartozik, amely a gerinchálózatot képviseli. Ez az OSPF-hálózat központi része, amely minden adatforgalmat kezel és irányít az egyes helyszínek között.

Minden egyéb hálózati terület, beleértve a Győr és Pozsony, Sopron helyszíneket is, az **Area 1**-hez tartozik. Ez a szegmentáció biztosítja, hogy az adatok optimálisan és hatékonyan eljutását a célállomásra, miközben minimalizálják a hálózati torlódásokat és javítják a teljesítményt.

angol:

The configuration and implementation of a VPN (Virtual Private Network) are essential for secure communication between the internal networks of the two organizations. The communication between the Sopron server and the Bratislava server is achieved through a VPN connection.

The dynamic traffic management of the network is achieved using the OSPF (Open Shortest Path First) protocol. Each site has a border router, which acts as a distribution point (backbone) and belongs to Area 0, representing the backbone network. This is the central part of the OSPF network, handling and directing all data traffic between the various locations.

All other network areas, including Győr, Bratislava, and Sopron, belong to Area 1. This segmentation ensures that data reaches its destination optimally and efficiently, while minimizing network congestion and improving performance.

10. dia

**Virtuális magánhálózat (VPN)**

A Virtuális Magánhálózat (VPN) egy privát hálózat kiterjesztése egy nyilvános hálózaton keresztül, lehetővé téve a felhasználók számára, hogy adatokat küldjenek és fogadjanak, mintha eszközeik közvetlenül kapcsolódnának a privát hálózathoz

A VPN-ek biztonságos hozzáférést biztosítanak a vállalat hálózatához távoli helyszínekről, biztosítva, hogy az érzékeny adatok védve legyenek az átvitel során. Ezt titkosítási protokollok segítségével érik el, amelyek megvédik az adatokat, hogy azok olvashatatlanok legyenek az illetéktelen felhasználók számára. Az otthonról vagy más távoli helyszínekről dolgozó alkalmazottak biztonságosan csatlakozhatnak a vállalat belső hálózatához, hozzáférve erőforrásokhoz, mint például fájlok, alkalmazások és adatbázisok, mintha fizikailag jelen lennének az irodában​

Belső szabályzat alapján a soproni és a pozsonyi szerver között biztonságosabb VPN kapcsolat lett kialakítva.

A leadott vizsgaremek tartalmaz egy videót a működéséről az idő rövidsége miatt nem kívánjuk ezt most levetíteni.

vpn

AES 256-bites titkosítás

IPsec és ISAKMP

Sh crypto ipsec sa

11.dia

### Tűzfal

A tűzfalak a hálózati biztonság kritikus elemei, amelyek akadályt képeznek a megbízható belső hálózatok és a megbízhatatlan külső hálózatok, például az internet között. Felügyelik és szabályozzák a bejövő és kimenő hálózati forgalmat az előre meghatározott biztonsági szabályok alapján.

A Szálkapari Zrt.-nél a tűzfal egy 5506-X ASA1 egy típusú készülékkel lett megvalósítva. (Adaptive Security Appliance) . A két irányú forgalmat a definiált szabályok alapján szűri, korlátozza.

A tűzfal jelenlegi állapotában két szabályt tartalmaz. Egyik a ping átengedése, ez egy ideiglenes megoldás a tesztelés érdekében. Illetve 443-as https forgalom van engedélyezve.