



Vybrané kapitoly zo siet'ovej bezpečnosti II.

(Vzdelávanie pre zamestnancov verejnej správy v kategórii
používateľov „IT manažér“, „informatik“, „zamestnanec v
kybernetickej bezpečnosti“ – modul č. 3)

Meno a priezvisko

XX.XX.XXXX



KC KB UPJŠ

<https://cyberawareness.sk/>

The screenshot shows the homepage of the KC KB UPJS website. At the top left, there are logos for KCKB UPJS and CSIRT UPJS. To the right, there is a navigation menu with links for 'O projekte', 'Aktivity', 'Vzdelávanie', and 'Informácia o konaní vzdelávacích aktivít', along with a language selector for 'EN' and a search icon. The main content area features a dark blue background with a glowing shield and padlock icon on the left. The central text reads 'Vitajte na oficiálnom webovom sídle KC KB na UPJŠ'. Below this, there are logos for the European Union (financed by the NextGenerationEU program) and the Ministry of Investment, Regional Development and Information of the Slovak Republic. At the bottom, there are four blue buttons with icons and text: 'Expertná činnosť' (with a hand holding a pencil), 'Výskum' (with a magnifying glass), 'Vzdelávanie' (with three medals), and 'Spolupráca' (with two hands shaking).



Vzdelávacia aktivita (I.)

- Časový harmonogram
 - 08:30 – 10:00 – 1. blok
 - 10:00 – 11:30 – 2. blok
 - 11:30 – 12:30 – obedňajšia prestávka
 - 12:30 – 14:00 – 3. blok
 - 14:00 – 15:30 – 4. blok



PLÁN [OBNOVY]



Vzdelávacia aktivita (II.)

Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	Úvod do KIB a riadenie KIB	8	Online / Prezenčne
Modul č. 2	Vybrané kapitoly z kryptografie	8	Prezenčne
Modul č. 3	Vybrané kapitoly zo sieťovej bezpečnosti	16	Prezenčne
Modul č. 4	Reaktívne a proaktívne činnosti	8	Prezenčne
Modul č. 5	Reaktívne činnosti – komunikácia	6	Prezenčne
Modul č. 6	Vybrané kapitoly z práva informačných a komunikačných technológií I.	8	Online / Prezenčne
Modul č. 7	Vybrané kapitoly z práva informačných a komunikačných technológií II.	8	Online / Prezenčne



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MikroTik ako smerovač

IPv4 a IPv6 adresovanie



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ako sme na tom:

IPv4, IPv6, brána, maska, prefix, NW, BC, Host, delenie sietí?



IPv4 adresy na rozhranie

- IP → Addresses → +
- Vyplníme žiadanú adresu vrátane prefixu





IPv6 adresy na rozhranie

- IPv6 → Addresses → +
- Vyplníme žiadanú adresu vrátane prefixu





Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Smerovanie



Smerovanie

- Preposielanie paketov medzi sieťami
- Typy smerovania
 - Statické
 - Dynamické
 - Hybridné



PLÁN [OBNOVY]





Statické smerovanie

- Pevne zadané cesty
- Konfiguruje administrátor
- Lepšia kontrola nad dátovými tokmi
- Neschopnosť sa prispôbiť zmenám v topológii (výpadok linky)



PLÁN [OBNOVY]





Typy statických ciest

- Klasická
- Predvolená
- Sumarizačná
- Plávajúca



PLÁN [OBNOVY]



Statické smerovanie

Výhody

- Vyššia bezpečnosť
 - Kontrola nad trasou paketov
- Nižšia záťaž pre smerovač

Nevýhody

- Náročnejšia konfigurácia
 - Veľké/komplikované topológie
- Neprispôsobí sa zmene v topológii (výpadok linky)



Dynamické smerovanie

- Cesty nie sú pevne dané
- Spustený smerovací protokol
 - metrika
- Jednoduchšia konfigurácia
- Schopnosť sa prispôbiť zmenám v topológii (výpadok linky)



PLÁN [OBNOVY]



Dynamické smerovanie

Výhody

- Jednoduchšia konfigurácia a škálovanie siete
- Prispôsobenie sa zmenám v topológii

Nevýhody

- Vyššia záťaž pre smerovač
- Nižšia bezpečnosť



Metrika

- Hodnota cesty



PLÁN [OBNOVY]





Administratívna vzdialenosť

- Dôveryhodnosť cesty



PLÁN [OBNOVY]



Aktivita – statické smerovanie



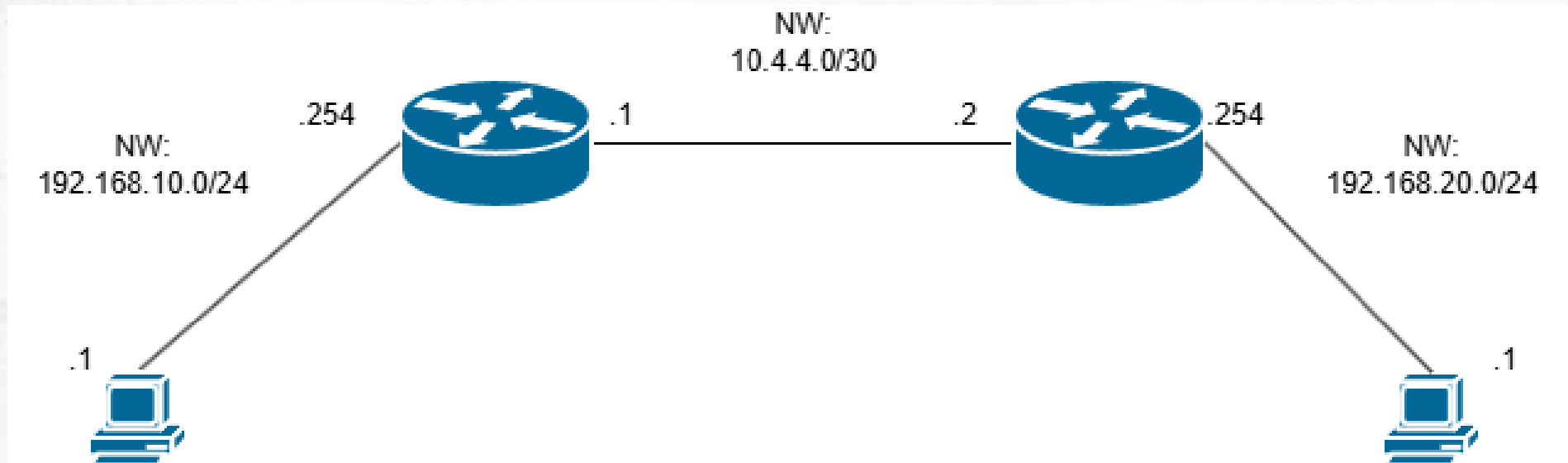
Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Topológia





Konfigurácia klasickej statickej cesty

- IP → Routes → +
- Dst. Address – adresa neznámej siete vrátane prefixu
- Gateway – next-hop adresa





Konfigurácia defaultnej statickej cesty

- IP → Routes → +
- Dst. Address – 0.0.0.0/0
- Gateway – next-hop adresa





Konfigurácia plávajúcej statickej cesty

- IP → Routes → +
- Dst. Address – adresa neznámej siete vrátane prefixu
- Gateway – next-hop adresa
- Metric - nastavíme na hodnotu 2



Aktivita – dynamické smerovanie IPv4



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Pridávame rozhrania v OSPF

- Routing → OSPF → karta Interfaces → +
- Vyberieme a pridáme použité rozhrania





Pridávame siete v OSPF

- Routing → OSPF → karta Networks → +
- Zadáme postupne všetky siete, ktoré smerovač pozná (vrátane prefixu)
- Vyberieme oblasť (ak realizujeme Multi Area OSPF)



Aktivita – dynamické smerovanie IPv6



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Nastavujeme Inštanciu v OSPFv3

- Routing → OSPFv3 → karta Instances → +
- Name - názov
- Router ID - identifikátor smerovača (tvar IPv4 adresy, unikátny)





Nastavujeme Inštanciu v OSPFv3

- Redistribute Connected Routes - as type 1



PLÁN [OBNOVY]





Pridávame rozhrania v OSPFv3

- Routing → OSPFv3 → karta Interfaces → +
- Pridáme postupne všetky použité rozhrania



Aktivita – kam príde Hello paket?



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Zabezpečenie pomocou Passive Interface

- Routing → OSPF → karta Interfaces → 2x LTM na kritické rozhranie
- Zaškrtne Passive



PLÁN [OBNOVY]





Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Aktivita – MITM útok



Realizujeme MITM útok

Bridge → karta Bridge → +

- Vytvoríme bridge

Karta Ports → +

- Do bridge pridáme rozhrania (3)



PLÁN [OBNOVY]





Realizujeme MITM útok

Switch → Settings → 2x LTM na switch

- Mirror Target – rozhranie k našemu PC
- Mirror Source – jedno z 2 ďalších v bridge



Aktivita – MITM a dynamické smerovanie



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Filtrovanie paketov



Access Control List

- Mechanizmus na základné filtrovanie paketov (L3 filter)
- Dva typy
 - Štandardný - filtrovanie akýchkoľvek paketov
 - Rozšírený - filtrovanie aj na základe služieb (portov)



PLÁN [OBNOVY]





Parametre pre nastavenie ACL v MikroTik-u

- Chain
- Zdrojová IP adresa
- Cieľová IP adresa
- Zdrojový port
- Cieľový port
- Akcia



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Chains v ACL

- **Input** – paket vstupuje do MikroTik-u a ostáva v ňom (MT bol jeho cieľ)
- **Output** – paket odchádza z MikroTik-u (MT bol jeho zdroj)
- **Forward** – paket prechádza MikroTik-om



PLÁN [OBNOVY]





Tipy pre nastavenie ACL

- ACL je zoznam (prechádza sa zhora nadol)
- Možné prístupy
 - Zakážem, čo potrebujem a ostatné povolím
 - Povolím, čo potrebujem a ostatné zakážem
- Ideálne čo najmenej pravidiel



PLÁN [OBNOVY]





Akcie v MikroTik ACL

- Accept - prepustí paket
- Drop - zahodí paket
- Reject – odmietne paket (odošle spätn väzbu, prečo bol paket odmietnut)



PLÁN [OBNOVY]



Aktivita – Filtrovanie paketov na L3



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

VPN



Definícia

- Spôsob realizácie zabezpečenej komunikácie prostredníctvom nezabezpečenej infraštruktúry
- Maskovanie geografickej polohy
- Zabezpečené prehliadanie internetu
- Skrývanie sieťovej (internetovej) aktivity



PLÁN [OBNOVY]





Použitie VPN

- Bezpečný prístup do firemného intranetu cez internet
- Maskovanie geografickej polohy
- Zabezpečené prehliadanie internetu
- Skrývanie sieťovej (internetovej) aktivity
- ...



PLÁN [OBNOVY]



Realizácia VPN

Client – Site VPN

- Pripojenie jedného koncového zariadenia k VPN serveru
- Nutná prítomnosť VPN klientskej aplikácie (vstavaná alebo Third-Party)

Site – to – Site VPN

- VPN tunel medzi dvoma smerovačmi
- Pobočky firiem a pod.
- Potrebná konfigurácia oboch smerovačov + úprava smerovania



VPN protokoly

- PPTP
- L2TP
- SSTP
- OVPN



PLÁN [OBNOVY]





Point-to-Point Tunneling Protocol

- Najstar
- Široká kompatibilita
- Jednoduché nasadenie a konfigurácia
- Slabá bezpečnosť (prelomiteľný rádovo v hodinách/dňoch)
- Tendencia upúšťania od podpory (Android, iOS)



PLÁN [OBNOVY]





Layer 2 Tunneling Protocol

- Široká kompatibilita
- Jednoduché nasadenie a konfigurácia
- Sám o sebe bez šifrovania
 - Nasadenie s nábstavbou IPsec





Secure Socket Tunneling Protocol

- Microsoft proprietary
- Zabezpečenie pomocou certifikátov
- Bezpečný
- Problematická kompatibilita



PLÁN [OBNOVY]





Open VPN

- Vysoká bezpečnosť
- Náročné nasadenie
- Slabá podpora v OS
 - Nutná Third-party aplikácia
 - Nutná



PLÁN [OBNOVY]



Aktivita – Konfigurácia VPN (klient - server)



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Nastavenie ARP na rozhraní

- Interfaces → 2x LTM na rozhranie brány
→ karta General
- ARP nastavíme na proxy-arp
- Gateway – next-hop adresa





Adresy pre VPN klientov

- IP → Pool → +
- Name - názov pool-u
- Addresses – rozsah adries z privátnej siete pre VPN klientov (syntax: prváIP-poslednáIP)





Nastavenie VPN profilu

- PPP → karta Profiles → +
- Name - názov VPN profilu
- Local Address – IP adresa brány
- Remote Address – vyberieme vytvorený pool





Nastavenie VPN profilu

- Use Compression – podľa potreby
- Use Encryption - yes





Nastavenie VPN profilu

- DNS Server – IP adresa brány
- Karta Protocols
- Use IPv6 - podľa potreby
 - Use MPLS – default





Vytvorenie VPN klienta

- PPP → karta Secrets → +
- Name – prihlasovacie meno
- Password – heslo
- Service – vyberieme požadovaný protokol



PLÁN [OBNOVY]





Vytvorenie VPN klienta

- Profile – vyberieme vytvorený profil



PLÁN [OBNOVY]





Spustenie VPN servera (PPTP/L2TP bez IPsec)

- PPP → karta Interface → LTM na požadovaný server
- Default Profile – vyberieme vytvorený profil
- Authentication – kompatibilita/to najlepšie
- Zaškrtneme Enable





Spustenie VPN servera (L2TP s IPsec)

- PPP → karta Interface → LTM na požadovaný server
- Default Profile – vyberieme vytvorený profil
- Authentication – kompatibilita/to najlepšie
- Zaškrtneme Enable





Spustenie VPN servera (L2TP s IPsec)

- PPP → karta Interface → LTM na požadovaný server
- Default Profile – vyberieme vytvorený profil
- Authentication – kompatibilita/to najlepšie
- Use IPsec - yes





Spustenie VPN servera (L2TP s IPsec)

- IPsec Secret – šifrovací kľúč (heslo)
- Use IPsec – yes
- Zaškrtneme Enable





Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Aktivita – Konfigurácia VPN (site to site)



MikroTik ako VPN klient

- Nastavenie VPN profilu
- Nastavenie pripojenia



PLÁN [OBNOVY]





Nastavenie VPN profilu

Karta Protocols

- Use IPv6 - podľa potreby
- Use MPLS – default
- Use Compression - podľa potreby
- Use Encryption - yes



PLÁN [OBNOVY]





Nastavenie VPN pripojenia

- PPP → karta Interface → + → vyberieme klienta podľa protokolu

Karta General

- Name – názov VPN virtuálneho rozhrania



PLÁN [OBNOVY]





Nastavenie VPN pripojenia

Karta Dial-out

- Connect to – vonkajšia IP VPN servera
- User – prihlasovacie meno
- Password – heslo
- Profile – vyberieme vytvorený profil



PLÁN [OBNOVY]





Nastavenie VPN pripojenia

Karta Dial-out

- Connect to – vonkajšia IP VPN servera
- User – prihlasovacie meno
- Password – heslo
- Profile – vyberieme vytvorený profil



PLÁN [OBNOVY]





Presmerovanie komunikácie do VPN tunela



PLÁN [OBNOVY]



Aktivita – Konfigurácia VPN – OpenVPN



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Pracovný list



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

✉ meno.priezvisko@upjs.sk

🌐 <https://cyberawareness.sk>