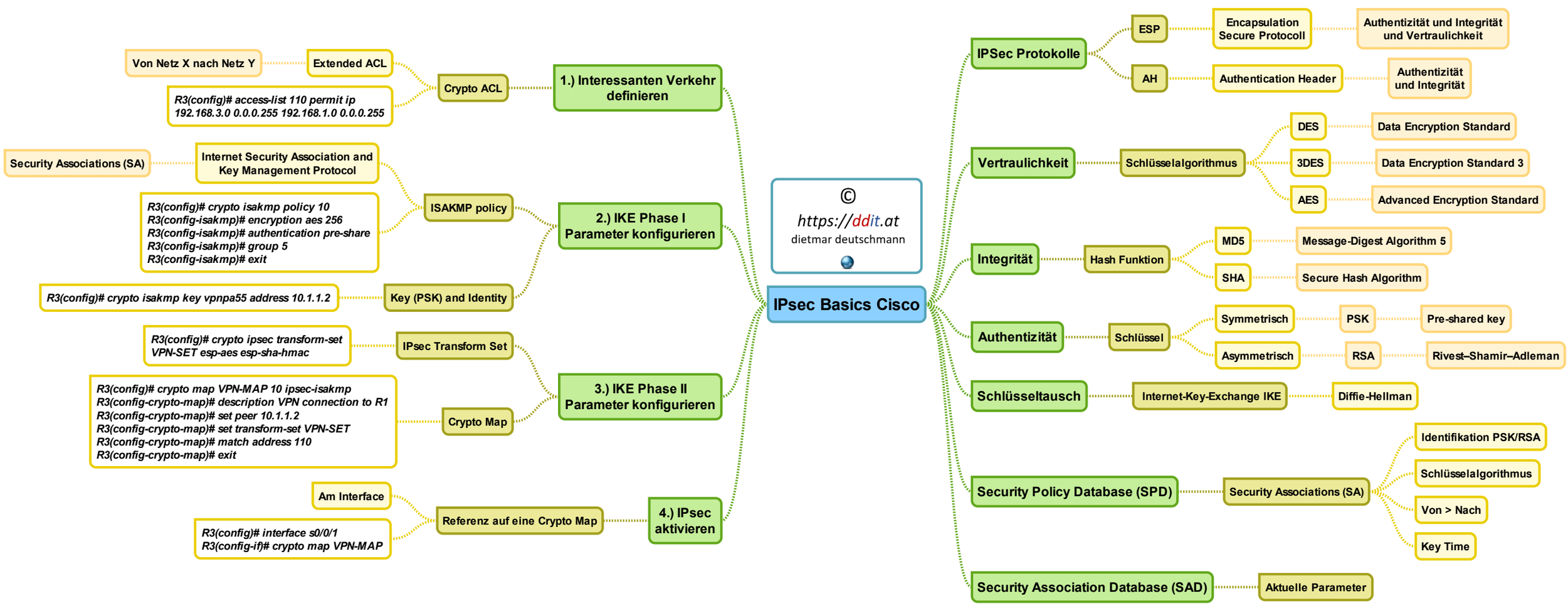
IPsec Basics Cisco
© https://ddit.at dietmar deutschmann
1.) Interessanten Verkehr definieren
Crypto ACL
Extended ACL
Von Netz X nach Netz Y
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
2.) IKE Phase I Parameter konfigurieren
ISAKMP policy
Internet Security Association and Key Management Protocol
Security Associations (SA)
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
Key (PSK) and Identity
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
3.) IKE Phase II Parameter konfigurieren
IPsec Transform Set
R3(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
Crypto Map
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
4.) IPsec aktivieren
Referenz auf eine Crypto Map
Am Interface
R3(config)# interface s0/0/1
R3(config-if)# crypto map VPN-MAP
IPSec Protokolle
ESP
Encapsulation Secure Protocoll
Authentizität und Integrität und Vertraulichkeit
AH
Authentication Header
Authentizität und Integrität
Vertraulichkeit
Schlüsselalgorithmus
DES
Data Encryption Standard
3DES
Data Encryption Standard 3
AES
Advanced Encryption Standard
Integrität
Hash Funktion
MD5
Message-Digest Algorithm 5
SHA
Secure Hash Algorithm
Authentizität
Schlüssel
Symmetrisch
PSK
Pre-shared key
Asymmetrisch
RSA
Rivest–Shamir–Adleman
Schlüsseltausch
Internet-Key-Exchange IKE
Diffie-Hellman
Security Policy Database (SPD)
Security Associations (SA)
Identifikation PSK/RSA
Schlüsselalgorithmus
Von > Nach
Key Time
Security Association Database (SAD)
Aktuelle Parameter