Technické požadavky a doporučení

pro členy federace eduroam.cz

verze 2017-06-03

Čl. 1 Společné požadavky pro poskytovatele identit (IdP) a poskytovatele zdrojů (SP)

1.1. Musí implementovat RADIUS server pro komunikaci s eduroam.cz infrastrukturou (RFC 2865).

1.2. Musí implementovat bezpečné propojení s eduroam.cz infrastrukturou. Preferován je RadSec (RFC 6614), alternativou je IPsec v transportním režimu na veřejných IPv4 adresách. Musí zajistit že RADIUS provoz nebude mimo síť instituce přenášen nešifrovaně, s výjimkou monitorovacího provozu.

1.3. Musí o zpracovaných autentizačních požadavcích logovat a minimálně 6 měsíců uchovávat alespoň následující informace:

- SP&IdP: časová značka
- SP&IdP: vnější EAP identita (tj. obsah atributu User-Name)
- IdP: vnitřní EAP identita (tj. skutečný identifikátor uživatele)
- SP&IdP: MAC adresa spojená s požadavkem o ověření (atribut Calling-Station-Id)
- SP&IdP: CUI (atribut Chargeable-User-Identity, IdP pokud je generováno, SP pokud bylo přijato)
- SP&IdP: výsledek autentizačního požadavku (Accept, Reject)
- SP: Je-li použit překlad síťových adres či portů (NAT/PAT), je třeba uchovávat i informace o jednotlivých překladech včetně časových značek.

1.4. Musí odpovídat na ICMP Echo Requests odeslané z národního RADIUS serveru a monitorovacího serveru.

1.5. Musí přijímat RADIUS požadavky na UDP/1812 z monitorovacího serveru.

1.6. Měl by podporovat Server-Status RADIUS požadavek (RFC 5997).

1.7. Musí mít čas synchronizovaný z kvalitního zdroje času.

1.8. Musí poskytovat úplné a aktuální informace o pokrytí podle požadavků eduroam databáze. Jedná se především o GPS souřadnice pokrytých lokalit a parametry poskytovaného připojení.

Čl. 2 Požadavky na eduroam IdP

2.1. Realm musí být doména nebo poddoména registrovaná v systému DNS. Doména by měla být vlastněna organizací provozující IdP.

2.2. Pokud není realm v CZ TLD musí implementovat NAPTR a SRV záznamy v DNS směrující RadSec požadavky na národní RADIUS server.

2.3. Musí implementovat EAP protokol (RFC 3580) pro ověřování uživatelů. Zvolená EAP metoda musí zajišťovat oboustranné ověření klienta a serveru a musí zajištovat end-to-end ochranu uživatelských kredencí.

2.4. Nesmí umožnit tunelování vnitřní EAP identity na jiný realm, tzv. test VCELKA-MAJA.

2.5. Měl by vynucovat shodu vnitřní a vnější identity, tzv. test FAKE-UID.

2.6. Může umožňovat použití anonymní identity ve tvaru anonymous@<realm> pokud implementuje Chargeable-User-Identity.

2.7. Měl by implementovat Chargeable-User-Identity. V případě, že implementuje Chargeable-User-Identity, tak musí zajistit, že pro konkrétní SP bude vždy generovat stejnou hodnotu a to i v případě, že uživatel může měnit vnější identitu. (např. několik různých realmů). (RFC 7593)

Čl. 3 Požadavky na eduroam SP

3.1. Musí posílat Access-Request pakety buď lokálně příslušnému RADIUS serveru té samé organizace které patří IdP anebo příslušnému nadřazenému RADIUS serveru.

3.2. Musí v Access-Requestech posílat atribut Calling-Station-Id a ten musí obsahovat MAC adresu zařízení ze kterého se uživatel připojuje.

3.3. Měl by odesílat atribut Operator-Name a pokud odesílá musí mít hodnotu 1<realm>. Pokud SP obsluhuje více institucí je odesílání Operator-Name povinné a musí být zajištěno odesílání pravdivé informace, pokud je možno fyzicky oddělit prostory institucí. (RFC 7593)

3.4. Měl by odesílat atribut Chargeable-User-Identity s hodnotou 0x00 (tj.požadovat CUI), pokud odesílá Operator-Name a pokud CUI umí zpracovat.

3.5. Neměl by posílat Accounting.

3.6. IEEE 802.11 WiFi síť musí vysílat essid SSID “eduroam”. Pokud je více než jedno eduroam SP v té samé lokalitě, je možné je odlišit pomocí prefixu “eduroam-” doplněným vhodnou zkratkou příslušné organizace jako doplněk k SSID “eduroam”. Je doporučeno aby se organizace domluvily a WiFi infrastrukturu sdílely.

3.7. IEEE 802.11 WiFi síť musí podporovat šifrování WPA2+AES a případně lepší.

3.8. Měl by poskytovat routovatelnou IPv4 adresu. Pro automatickou konfiguraci IPv4 adresy a rekurzivního DNS serveru musí být použit protokol DHCP.

3.9. Měl by poskytovat routovatelné IPv6 adresy přidělované mechanizmem bezestavové autokonfigurace (SLAAC).

3.10. Provoz uživatelů by neměl být filtrován, pokud k omezování v odůvodněných případech dochází, musí být otevřeny minimálně porty:

Služba	**Protokol/Port**
HTTP	TCP/80 TCP/443 TCP/3128 TCP/8080
Mail	TCP/465 TCP/587 TCP/143 TCP/993 TCP/110 TCP/995
FTP	TCP/20 TCP/21
SSH	TCP/22
Cisco IPSec VPN over TCP	TCP/10000
OpenVPN 2.0	UDP/1194
IPSec NAT-Traversal	UDP/4500
Standard IPSec VPN	IP protokol 50 (ESP) IP protokol 51 (AH) UDP/500 (IKE)
IPv6 Tunnel broker service	IP protokol 41
PPTP VPN	IP protocol 47 (GRE) TCP/1723

Nefunkčnost služby v případě, že je způsobena výhradně použitím překladu adres (NAT/PAT), není v rozporu s tímto ustanovením.

3.11. Důrazně se nedoporučuje implementace HTTP proxy, a pokud jsou použity, nesmí být využity ke sběru osobních údajů před umožněním přístupu k Internetu. Jejich implementace musí být zdokumentována na stránkách pro návštěvníky s URL dostupným prostřednictvím eduroam databáze.

3.12. Za **méně závažné** bezpečnostní incidenty se považuje prosté spamování, projevy nedokonalé konfigurace zařízení, zavirování počítače, bot, scanování apod.

3.13. Při řešení **méně závažných** bezpečnostních incidentů by se SP měl snažit co nejméně omezit uživatele, tj. lze-li předpokládat, že zdroj bezpečnostního incidentu je způsoben např. zavirovaným uživatelským zařízením. V takovém případě by SP měl blokovat pouze uživatelské zařízení pomocí MAC adresy. O zablokování MAC adresy zařízení a samotném bezpečnostním incidentu musí SP informovat organizaci (IdP), které přísluší uživatel zodpovědný za zablokované zařízení.

3.14. Za **závažné bezpečnostní** incidenty považujeme takové incidenty, kdy:

- prokazatelně dochází k narušování provozu sítě SP (spoofing, záplavové útoky, provozování zařízení v režimu síťového prvku apod.)
- prokazatelně je pozorována činnost, která může vést k narušení bezpečnosti sítě, k provozním problémům a jedná-li se útoky na jiné uživatele (lámání hesel, zneužití zařízení k amplifikačním útokům, řídící prvek botnetu, spam-phishingová kampaň apod.)
- prokazatelně narušuje legislativu ČR
- prokazatelně dochází k porušování politiky eduroam, například sdílením jedné eduroam identity mezi více uživateli

3.15. Při řešení **závažných** bezpečnostních incidentů je nutné zohlednit fakt že uživatelé mohou MAC adresy svých zařízení měnit. Pak je pro SP výhodnější blokovat uživatele na základě jeho vnější EAP identity a ideálně za pomocí Chargeable-User-Identity, kterou uživatel nemůže ovlivnit. O zablokování uživatele a souvisejícím bezpečnostním incidentu musí SP informovat organizaci (IdP) které přísluší uživatel identifikovaný jako původce incidentu.

3.16. Pokud IdP nepodporuje Chargeable-User-Identity, anebo nevynucuje shodu vnitřní a vnější identity, může SP při řešení a předcházení **závažným** bezpečnostním incidentům přistoupit k blokování celého realmu. O zablokování realmu musí SP informovat organizaci provozující IdP a operátora eduroam federace.

3.17. Při řešení bezpečnostních incidentů v rámci ČR komunikují správci SP se správci IdP napřímo, kontaktní informace získávají z databáze provozované operátorem federace.

3.18. Při řešení bezpečnostních incidentů přesahujících ČR komunikaci se doporučuje komunikovat prostřednictvím vlastního bezpečnostního týmu a pokud ho organizace nemá, tak prostřednicttvím CESNET-CERTS: certs@cesnet.cz, http://csirt.cesnet.cz.

Čl. 4 Požadavky na proxy RADIUS

4.1. Proxy RADIUSem je myšlen RADIUS server, který pouze zprostředkovává komunikaci RADIUS serverům z organizací a nebo organizačních jednotek s národním RADIUSem.

4.2. Musí zajistit odesílání pravdivě vyplněného atributu Operator-Name. V případě organizačních jednotek té samé organizace musí odesílat Operator-Name s

realmem organizační jednotky, jen pokud je tato organizační jednotka registrována u národního operátora federace.

4.3. Musí zajistit odesílání rozšířených statistických dat F-Ticks operátorovi národní eduroam federace. V případě organizačních jednotek té samé organizace musí zajistit odesílání F-Ticks, jen pokud je tato organizační jednotka registrována u národního operátora federace.

4.4. Musí zajistit že nepošle na národní RADIUS požadavek s realmem který přísluší některému z RADIUS serverů zapojených pod ním. Musí zajistit že to neudělá ani žádný ze serverů k němu připojených pokud tyto mají přímé spojení s národním RADIUSem.