ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

TARMOQ ADMINISTRATORLARI FAOLIYATINI NAZORAT QILISHDA TACACS+ ASOSIDAGI MONITORING TIZIMINI LOYIHALASH VA AMALIY JORIY ETISH TAJRIBALARI

Alimatov Bekmurod Olimjon o'g'li
University of Management and Future Technologies
Kommunikatsiya va Raqamli Texnologiyalar Kafedrasi Magistranti.
https://doi.org/10.5281/zenodo.15429031

Annotatsiya. *Ushbu maqolada tarmoq administratorlari tomonidan amalga oshiriladigan harakatlarni aniq qayd etish, ularni kuzatish va tahlil qilish maqsadida TACACS+ (Terminal Access Controller Access-Control System Plus) protokoli asosida monitoring tizimini loyihalash va amaliyotga joriy etish tajribalari ko‘rib chiqiladi. TACACS+ orqali markazlashtirilgan autentifikatsiya, avtorizatsiya va hisobga olish (AAA) xizmatlari yordamida tarmoq xavfsizligini ta’minlashning texnik va tashkiliy jihatlari yoritiladi.*

Kalit so‘zlar: *TACACS+, tarmoq xavfsizligi, AAA, monitoring tizimi, autentifikatsiya, avtorizatsiya, hisobga olish, nazorat qilish, administrator faoliyati.*

ОПЫТ ПРОЕКТИРОВАНИЯ И ВНЕДРЕНИЯ СИСТЕМЫ МОНИТОРИНГА НА БАЗЕ TACACS+ ДЛЯ КОНТРОЛЯ ДЕЯТЕЛЬНОСТИ СЕТЕВЫХ АДМИНИСТРАТОРОВ

Аннотация. *На данной статье рассматривается опыт проектирования и внедрения системы мониторинга на основе протокола TACACS+ (Terminal Access Controller Access-Control System Plus) для точной регистрации, отслеживания и анализа действий, предпринимаемых сетевыми администраторами. Рассматриваются технические и организационные аспекты обеспечения безопасности сети с использованием централизованных служб аутентификации, авторизации и учета (AAA) через TACACS+.*

Ключевые слова: *TACACS+, сетевая безопасность, AAA, система мониторинга, аутентификация, авторизация, учет, контроль, действия администратора.*

EXPERIENCES IN DESIGNING AND IMPLEMENTING A MONITORING SYSTEM BASED ON TACACS+ TO MONITOR THE ACTIVITIES OF NETWORK ADMINISTRATORS

Abstract. *This article reviews the experiences in designing and implementing a monitoring system based on the TACACS+ (Terminal Access Controller Access-Control System Plus) protocol in order to accurately record, monitor, and analyze the actions taken by network administrators. The technical and organizational aspects of ensuring network security using centralized authentication, authorization, and accounting (AAA) services through TACACS+ are covered.*

Keywords: *TACACS+, network security, AAA, monitoring system, authentication, authorization, accounting, control, administrator activities.*

Kirish

Zamonaviy axborot-kommunikatsiya infratuzilmasida tarmoq administratorlarining roli beqiyosdir. Ular tarmoqning uzluksiz ishlashi, xavfsizligi va samaradorligini ta’minlash uchun

mas’ul bo‘lib, router, switch, server va boshqa qurilmalarga doimiy tarzda kirish huquqiga ega bo‘ladilar. Biroq, bu imkoniyatlar tarmoq xavfsizligi nuqtai nazaridan muayyan xatarlarni yuzaga keltiradi: noto‘g‘ri konfiguratsiyalar, tasodifiy yoki ataylab bajarilgan xavfli buyruqlar, ruxsatsiz o‘zgartirishlar va axborotlar sizib chiqishi kabi tahdidlar mavjud.

Aksariyat hollarda, administratorlar tomonidan bajarilgan harakatlar bo‘yicha markazlashtirilgan nazorat va auditning mavjud emasligi, xavfsizlik insidentlarini aniqlash va tahlil qilish imkonini sezilarli darajada cheklaydi. Shu sababli, tarmoq xavfsizligini ta’minlashda nafaqat tashqi tahdidlarga qarshi kurash, balki ichki faoliyat, ya’ni administratorlar ish faoliyatining shaffofligini ta’minlash ham muhim omil hisoblanadi.

Ushbu muammoning yechimi sifatida **TACACS+ (Terminal Access Controller Access-Control System Plus)** texnologiyasi asosida monitoring tizimini joriy etish mumkin. TACACS+ yordamida autentifikatsiya, avtorizatsiya va hisobga olish (AAA) funksiyalarini markazlashtirilgan holda amalga oshirish orqali administratorlarning har bir harakati aniqlik bilan qayd etiladi va tahlil qilinadi. Ushbu maqola aynan shunday tizimni texnik jihatdan loyihalash va amaliyotga joriy etish bo‘yicha tajribalarga bag‘ishlanadi.

TACACS+ texnologiyasi haqida qisqacha ma’lumot

TACACS+ – bu Cisco Systems tomonidan ishlab chiqilgan xavfsizlik protokoli bo‘lib, uchta asosiy xavfsizlik komponentini birlashtiradi:

1. **Autentifikatsiya (Authentication):** Foydalanuvchining (yoki administratorning) tizimga kirishga bo‘lgan huquqini tekshiradi. Bu bosqichda foydalanuvchi nomi va parol (yoki boshqa autentifikatsiya usuli) orqali identifikatsiya amalga oshiriladi.
2. **Avtorizatsiya (Authorization):** Kirishga ruxsat berilgach, foydalanuvchining qanday harakatlarni amalga oshirishi mumkinligi aniqlanadi. Bu bosqichda foydalanuvchi huquqlari – qaysi buyruqlarni bajarishi, qaysi qurilmalarga kirishi mumkinligi belgilanadi.
3. **Hisobga olish (Accounting):** Har bir foydalanuvchining tizimdagi faoliyati batafsil qayd etiladi. Bu loglar orqali qaysi foydalanuvchi qachon tizimga kirgani, qanday buyruqlar bajargani, qachon chiqib ketgani haqida ma’lumotlar olinadi.

TACACS+ ning afzalliklari:

- Har bir so‘rovni to‘liq shifrlaydi (RADIUSdan farqli ravishda).
- Buyruq-darajadagi avtorizatsiyani qo‘llab-quvvatlaydi.
- Mustaqil autentifikatsiya, avtorizatsiya va hisobga olish modullariga ega.
- Raqobatchi protokollarga qaraganda ko‘proq nazorat imkonini beradi.

Ushbu protokol ayniqsa yirik korporativ tarmoqlarda, davlat muassasalari va harbiy infratuzilmada qo‘llanilishi bilan mashhur.

Monitoring tizimini loyihalash bosqichlari

TACACS+ asosida monitoring tizimini yaratish bosqichma-bosqich yondashuvni talab qiladi. Quyida texnik jihatdan puxta o‘ylangan loyiha amaliyotga qanday joriy etilishi keltirilgan:

1. Tizim arxitekturasini aniqlash

Monitoring tizimi quyidagi asosiy komponentlardan tashkil topadi:

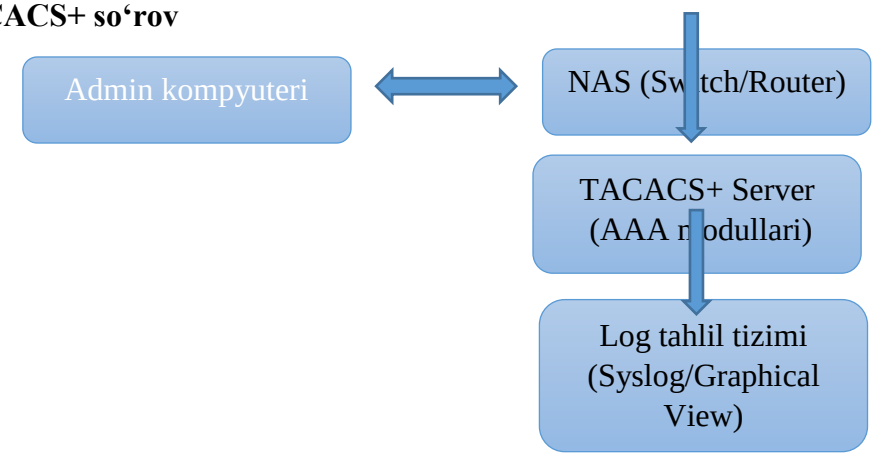
• **TACACS+ server (Markaziy AAA serveri):** Barcha autentifikatsiya, avtorizatsiya va hisobga olish jarayonlarini boshqaradi. Cisco ISE, FreeRADIUS (TACACS+ moduli orqali), yoki TACACS.net serverlari ishlatiladi.

• **NAS qurilmalar (Network Access Server):** Routerlar, switchlar va boshqa qurilmalar bo‘lib, foydalanuvchilar ushbu qurilmalarga kirishda TACACS+ serverga murojaat qiladi.

• **Administrator ishchi stansiyalari:** Administratorlar terminal yoki SSH orqali tarmoq qurilmalariga ulanadi.

TACACS+ asosidagi monitoring tizimi arxitekturasi

TACACS+ so‘rov



2. TACACS+ serverni o‘rnatish va sozlash

Server operatsion tizimiga (Linux, Windows) qarab quyidagilar bajariladi:

• FreeRADIUS kabi platformalarda tac_plus konfiguratsiya fayli yaratiladi.

• Har bir foydalanuvchi uchun autentifikatsiya ma’lumotlari belgilanadi.

• Hisobga olish (accounting) loglari uchun fayl yoki syslog konfiguratsiyasi o‘rnatiladi.

Masalan:

```
user = admin1 {
default service = permit
login = cleartext "password123"
cmd = show {
permit .*
}
cmd = configure {
permit interface
}
}
```

4. 3. NAS qurilmalarini konfiguratsiya qilish

Router yoki switchda quyidagi buyruqlar orqali TACACS+ serverga ulaniladi:

```
aaa new-model
tacacs-server host 192.168.100.10 key tacacssecret
aaa authentication login default group tacacs+ local
```

aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+

Bu sozlamalar orqali:

- Autentifikatsiya avval TACACS+ orqali, keyin lokal usulda amalga oshiriladi (agar birinchisi muvaffaqiyatsiz bo‘lsa).
- Buyruqlarni bajarish va sessiya boshqaruvi nazorat ostida bo‘ladi.
- Harakatlar logga yoziladi.

5. 4. Hisobga olish tizimini joriy qilish

- Har bir sessiya haqida loglar yaratiladi: kirish vaqti, bajarilgan buyruqlar, sessiya davomiyligi.
- Loglar markaziy syslog serverga uzatiladi yoki lokal fayllarda saqlanadi.
- Web interfeys orqali real vaqtli monitoring ham amalga oshiriladi (masalan, TACACS.net interfeysi).

6. 5. Sinov va audit

- Test foydalanuvchilari orqali tizimga kirish va harakatlar bajariladi.
- Audit jurnallari tekshiriladi va noto‘g‘ri konfiguratsiyalar aniqlanadi.
- Hisobotlar shakllantiriladi va xavfsizlik bo‘yicha tavsiyalar tayyorlanadi.

Amaliy joriy etish tajribalari

TACACS+ asosidagi monitoring tizimini sinovdan o‘tkazish maqsadida o‘rta hajmdagi oliy ta’lim muassasasining kampus tarmog‘ida tajriba loyihasi amalga oshirildi. Tarmoqda 12 ta router va 20 ta switch mavjud bo‘lib, ularni boshqaruvchi 5 nafar administrator faoliyat yuritardi.

Loyiha quyidagi bosqichlarda amalga oshirildi:

1. Pilot hudud tanlash

Kampusning ma’muriy qismi tajriba maydonchasi sifatida belgilandi. Bu hududdagi barcha router va switchlar TACACS+ tizimiga ulanib, audit qilish yo‘lga qo‘yildi.

2. Foydalanuvchi rollarini aniqlash

Har bir administrator uchun alohida foydalanuvchi hisobi yaratildi va quyidagi rollar berildi:

- **Tizim boshqaruvchisi** – barcha buyruqlarni bajarish huquqiga ega.
- **Texnik mutaxassis** – faqat ko‘rish va konfiguratsiya holatini o‘qish imkoniyatiga ega.
- **Sinov foydalanuvchisi** – cheklangan funksiyalar uchun.

3. Hisobga olish va tahlil qilish

Monitoring tizimi har bir foydalanuvchining:

- Kirish vaqtini,
- Qaysi qurilmaga ulanganini,
- Bajarilgan har bir buyruqni,
- Chiqqan vaqtini to‘liq log fayllarda qayd etdi.

4. Nazorat va ogohlantirish mexanizmlari

Tizimda quyidagi ogohlantirishlar o‘rnatildi:

- Soat 18:00 dan keyingi barcha kirishlar bo‘yicha ogohlantirishlar email orqali yuboriladi.
- “configure terminal” yoki “interface” kabi xavfli buyruqlar bajarilganda logda alohida flag qo‘yiladi.

Natijalar:

- Administratorlar faoliyati shaffof bo‘ldi, javobgarlik oshdi.
- Tarmoqdagi noto‘g‘ri sozlash holatlari aniqlandi va bartaraf qilindi.
- Tahlil natijalariga ko‘ra, 2 ta administrator tomonidan noto‘g‘ri buyruqlar bajarilgani aniqlanib, tegishli choralar ko‘rildi.

Xulosa

TACACS+ texnologiyasi asosida yaratilgan monitoring tizimi tarmoq xavfsizligini oshirishda, ichki foydalanuvchi faoliyatini kuzatishda va audit jarayonlarini avtomatlashtirishda samarali yechimdir. Bu tizim nafaqat administratorlarning harakatlarini real vaqt rejimida nazorat qilish, balki tarmoqdagi barcha jarayonlar ustidan to‘liq shaffoflikni ta’minlash imkonini beradi.

Maqolada keltirilgan tajriba asosida aytish mumkinki:

- TACACS+ orqali autentifikatsiya, avtorizatsiya va hisobga olish xizmatlarini markazlashtirish tarmoq xavfsizligiga muhim hissa qo‘shadi.
- Buyruq-darajadagi nazorat tarmoqdagi ruxsatsiz o‘zgarishlarni aniqlash imkonini beradi.
- Ogohlantirish va hisobot tizimlari esa xavfsizlik bo‘yicha tezkor qarorlar qabul qilishga yordam beradi.

Kelgusida ushbu tizimga sun’iy intellekt asosidagi log-tahlil mexanizmlari qo‘shilsa, harakatlar avtomatik tahlil qilinib, anomal xatti-harakatlar aniqlanishi mumkin bo‘ladi.

REFERENCES

1. Cisco Systems. *TACACS+ Protocol Specification*. Cisco Whitepapers.
2. RFC 8907 – *The Terminal Access Controller Access-Control System Plus (TACACS+)*. IETF.
3. FreeRADIUS Documentation – https://wiki.freeradius.org
4. Tanenbaum, A. S., Wetherall, D. J. *Computer Networks*, 5th Edition.
5. Stallings, W. *Network Security Essentials: Applications and Standards*, 6th Edition.
6. TACACS.net Server Documentation – https://tacacs.net/