TEXNIK TOPSHIRIQNOMA

«TASDIQLAYMAN»
“Biznesni rivojlantirish banki” ATB
Boshqaruv raisi o'rinbosari v.b:
B.Bobojonov

«25» may 2026 y.
№ 388

«Biznesni rivojlantirish banki» ATB da yangi avlod tarmoqlararo ekranlari (NGFW) majmuasini kengaytirish va yangilash bo‘yicha

Toshkent-2026

Mundarija

1. Hujjat rekvizitlari

Hujjat turi	Texnik topshiriq
Loyiha nomi	ATB «Biznesni rivojlantirish banki»da yangi avlod tarmoqlararo ekranlar (NGFW) kompleksini kengaytirish va yangilash
Buyurtmachi	«Biznesni rivojlantirish banki» ATB
Ijrochi	Tanlov natijalari bo‘yicha aniqlanadi

2. Loyihaning maqsadi va vazifalari

Hozirgi vaqtda Bankning filiallararo tarmog'i yagona tarmoq infratuzilmasiga birlashtirilgan va Bankning amaldagi filiallari hamda bo'linmalari o'rtasidagi aloqani ta'minlaydigan NGFW toifasidagi 43 ta qurilma asosida qurilgan.

Bankning mintaqaviy faoliyatini rivojlantirish va kengaytirish strategiyasiga muvofiq, yaqin kelajakda qo'shimcha filiallar va bo'linmalarni ulash rejalashtirilgan bo'lib, bu mavjud tarmoq infratuzilmasini kengaytirishni talab qiladi.

Quyidagilarni hisobga olgan holda:

- Bank filiallar tarmog'ining o'sish dinamikasi;
- axborot xavfsizligi va tarmoq arxitekturasining yagona standartlarini saqlab qolish zarurati;
- markazlashtirilgan boshqaruv, nosozliklarga chidamlilik va trafik nazoratiga qo'yilgan talablar;
- amaldagi uskunalar xavfsizligini uzluksiz ta'minlash maqsadida xavfsizlik obunalari va texnik qo'llab-quvvatlash xizmatlarini yangilab borish zarurati;
- filiallararo tarmoqni parchalanishiga va turli xil tarmoq yechimlaridan foydalanishga yo'l qo'yib bo'lmasligi,

tarmoqni kengaytirish uchun qo'shimcha tarmoq uskunalari sotib olish, amaldagi litsenziyalarni yangilash, shuningdek markazlashtirilgan boshqaruv tizimi imkoniyatlarini kengaytirish zarurati yuzaga kelmoqda.

Mazkur maqsadga erishish quyidagilarga imkon beradi:

- filiallararo tarmoq infratuzilmasini keyingi rivojlantirish va kengaytirish uchun apparat va dasturiy ta'minot bazasini yaratish;
- Bank uskunalar parkining uzluksiz ishlashini va kiberxavfsizlikning hozirgi darajasini kafolatlash;
- Bankning uzoq muddatli o'sishini qo'llab-quvvatlash uchun boshqariladigan qurilmalar soni bo'yicha zaxiraga ega markazlashtirilgan tarmoq boshqaruv tizimini ta'minlash;
- barcha ob'ektlarda axborot xavfsizligining yagona darajasini saqlab qolish;
- tarmoqni keyingi kengaytirishda operatsion va ekspluatatsion xatarlarni minimallashtirish;
- infratuzilmani sezilarli arxitekturaviy o'zgartirishlarsiz kengaytirish imkoniyatini ta'minlash.

3. Eng maqbul taklifni tanlashning texnik qismi

Yetkazib beriladigan mahsulot sifati texnik topshiriqda (bundan keyin TT deb ataladi) ko'rsatilgan talablarga muvofiq bo'lishi lozim.

Yetkazib beriladigan tovarlarning miqdori va hajmi hamda ko'rsatiladigan xizmatlar ko'lami TT ga muvofiq bo'lishi shart.

4. Tovarlarni yetkazib berish rejalashtirilgan muddatlari

5. Tovarlarni yetkazib berish muddati: yangi qurilmalar uchun shartnoma imzolangan kundan boshlab 90 kalendar kundan kechiktirmay, obunalarni uzaytirish uchun esa 20 kalendar kundan kechiktirmay.

6. Yetkazib berish manzili

Yetkazib berish manzili: Buyurtmachining ofisi, manzil: Toshkent sh., Navoiy ko‘chasi 18A.

7. NGFW qurilmalariga qo‘yiladigan texnik talablar

6.1. NGFW qurilmalarining funksional imkoniyatlariga qo‘yiladigan talablar

1. Seans holatini nazorat qiluvchi yangi avlod tarmoq devori (NGFW) bo‘lishi, OSI modeli bo‘yicha Layer-2 dan Layer-7 gacha ishlashi;
2. Tizim OSPF, OSPFv3, RIP, BGP va statik marshrutlar kabi marshrutlash protokollarini qo‘llab-quvvatlashi;
3. Tarmoqlararo ekran orqali o‘tuvchi trafik bo‘yicha OSI modeli Layer-7 darajasida tarmoq ilovalarini aniqlash va bloklash, shu jumladan umumiy portlardan foydalanadigan barcha ilovalar uchun (masalan, 80 va 443 portlar) va dinamik TCP/UDP portlaridan foydalanadigan barcha ilovalar uchun alohida;
4. Tarmoqlararo ekranda saqlanadigan signaturalar bo‘yicha OSI modelining Layer-7 qatlamida tekshirilayotgan trafikda quyidagi toifadagi ilovalarni aniqlash:
   - ✓ Korporativ ilovalar: autentifikatsiya xizmatlari, jumladan Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS; ma’lumotlar bazasini boshqarish tizimi, jumladan Microsoft SQL, Oracle, DB2, Postgres, Sybase; fayl xizmatlari, jumladan Microsoft SMB; ERP, CRM tizimlari, jumladan SAP, 1C; elektron hujjat aylanishi va xabar almashish tizimlari, jumladan EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus;
   - ✓ Elektron pochta almashish protokollari: SMTP, POP3, IMAP;
   - ✓ VoIP va audio-video konferensiya protokollari, jumladan SIP, H.323, H.245, H.225, Webex;
   - ✓ Dasturiy ta’minotni yangilash xizmatlari, jumladan Microsoft Update, antivirus dasturlari (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple;
   - ✓ Zaxira nusxa xizmatlari, jumladan Symantec Backup Exec;
   - ✓ Virtualizalashtirish va terminal kirish xizmatlari, jumladan VMware, Citrix, Microsoft RDP;
   - ✓ Taqsimlangan ilovalarni yaratish uchun qo‘llaniladigan boshqa protokollar va texnologiyalar, jumladan CORBA, SOAP;
   - ✓ Masofaviy kirish protokollari, jumladan Telnet, SSH, VNC, Radmin;;
   - ✓ Tarmoq protokollari, jumladan dinamik marshrutlash protokollari va SSL, IPsec VPN;
5. Internet tarmog‘i ilovalari:
   - ✓ Elektron pochta, jumladan Gmail, Yandex.Mail, Mail.ru, Hotmail;
   - ✓ Ijtimoiy tarmoqlar, jumladan Facebook, Google+, LinkedIn, VKontakte, Odnoklassniki, “Moy Mir”;

- ✓ Xabarlarni tezkor almashish vositalari, jumladan ICQ, Jabber, IRC, MSN, shuningdek yuqorida sanab o‘tilgan ijtimoiy tarmoqlardagi analog xizmatlar;
- ✓ Audio-video konferensiya vositalari, jumladan Skype;
- ✓ HTTP(S) va peer-to-peer orqali fayl almashish vositalari, jumladan Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, SkyDrive, WebDav;
- ✓ Oqimli audio-video (veb-saytdan qat’i nazar), jumladan YouTube, Vimeo, HTTP orqali audio va video;
- ✓ Team-Viewer, LogMeIn kabi ish stolini nashr etish va masofaviy kirish imkonini beruvchi vositalar;
- ✓ Tashqi proksi-serverlar va anonimlashtiruvchilar, jumladan Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy;
- ✓ Shaxsiy VPN yaratish va boshqa ilovalar ustida tunnellash vositalari, jumladan FreeNet, OpenVPN, VTun, RDP-to-TCP, TCP-over-DNS;

6. Tarmoqlararo ekran tarkibida HTTP(S), FTP, SMB, SMTP, RPC va boshqa protokollar dekoderlaridan foydalangan holda regulyar ifodalar asosida ilovalar uchun o‘z signaturalarini yaratish imkoniyatlarini taqdim etish, shuningdek TCP/UDP paketlari tarkibi bo‘yicha maska asosida signaturalar tuzish;
7. HTTP/2 protokoli orqali uzatilayotgan ilovalarni aniqlash;
8. SSL (RSA kalitlari 2048 bitgacha qo‘llab-quvvatlanadi) va SSHv2 shifrlangan trafik bo‘yicha tarmoq ilovalarini aniqlash: tarmoqlararo ekran orqali o‘tuvchi trafikni (SSL, SSHv2 deshifrlash) kiruvchi va chiquvchi ulanishlar uchun, domen foydalanuvchilari uchun shaffof tarzda, ilovalarning alohida funksiyalarini nazorat qilish imkoniyati bilan, jumladan ijtimoiy tarmoqlarda xabar yuborish, fayl almashish, oqimli audio va video;
9. Tunnel inspeksiyasi:
   - ✓ Generic Routing Encapsulation (GRE) (RFC 2784);
   - ✓ Shifrlanmagan IPSec trafik [NULL Encryption Algorithm for IPSec (RFC 2410)];
   - ✓ Transport rejimi AH IPSec.
10. Bir seans doirasida ishlatilayotgan turli ilovalarni ketma-ket aniqlash;
11. Tarmoq ilovalaridan foydalanuvchi foydalanuvchilarni aniqlash: Korporativ autentifikatsiya xizmatlari bilan integratsiya orqali, jumladan Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; boshqa autentifikatsiya xizmatlari (masalan, simsiz tarmoq boshqaruvchilari) bilan ochiq XML API orqali integratsiya qilish imkoniyati; foydalanuvchilarning majburiy avtorizatsiyasini WEB sahifa – “Captive portal” orqali ishlatish; Kerberos, Tacacs+, SAML v.2 qo‘llab-quvvatlash, foydalanuvchilarni L3 roaming yordamida WMI va NetBios so‘rovlar orqali qo‘llab-quvvatlash;
12. Tarmoqlararo ekran orqali uzatilayotgan trafik tarkibini signaturalar va xatti-harakatlar bo‘yicha real vaqt rejimida oqimda tekshirish, zaifliklar, tarmoq hujumlari va zararli dasturlardan himoya qilish, ularning signaturalari bo‘yicha fayl turlarini aniqlash, veb, elektron pochta, FTP, SMB orqali tarqatilayotgan viruslar va shaxsiy kuzatuv dasturlarini aniqlash, tarmoq qurtlarini aniqlash; SSL va SSHv2 shifrlangan ilovalar uchun ham, muayyan tarkibni bloklash, jumladan, muntazam ifodalar (regular expressions) yordamida;
13. Tarmoqlararo ekran orqali o‘tuvchi trafik uchun yagona xavfsizlik siyosatida qoidalar yaratish, har bir ulanishning quyidagi parametrlarini kvalifikator sifatida ishlatish:
   - ✓ Jo‘natuvchi IP-manzili,
   - ✓ Qabul qiluvchi IP-manzili,

- ✓ L4 darajasidagi ishlatilayotgan xizmatlar: TCP va UDP protokollari portlari,
- ✓ Active Directory foydalanuvchilari yoki foydalanuvchi guruhlarining nomlari,
- ✓ OSI modeli 7-darajasidagi ilovalar,
- ✓ URL kategoriyasi.

14. Yagona xavfsizlik siyosatida qoidalar yaratish, har bir ulanishning jo‘natuvchi va qabul qiluvchi IP-manzillari, ishlatilayotgan xizmatlar (TCP/UDP portlari), foydalanuvchi nomlari, foydalanuvchi guruhlari va foydalanuvchi yoki guruh tomonidan ishlatiladigan ilovalar yoki ma’lum ilova kategoriyalari ma’lumotlarini kvalifikator sifatida ishlatish. Yaratilayotgan siyosatlarda quyidagi amallarni bajarish imkoniyati bo‘lishi lozim:
    - ✓ Ruxsat berish yoki taqiqlash;
    - ✓ Ma’lum bir ilova yoki ilova kategoriyasiga faqat standart yoki qat’iy belgilangan TCP/UDP portlardan foydalanishga ruxsat berish. Shu bilan birga, ushbu portlar boshqa ilovalar tomonidan siyosatda ochiq ruxsat berilmagan holda ishlatilmasligi kerak;
    - ✓ Ruxsat berish, lekin virus va boshqa tahdidlar bo‘yicha skanerlashni amalga oshirish;
    - ✓ Ruxsat berish yoki taqiqlash, jadval, foydalanuvchi yoki foydalanuvchi guruhi asosida;
    - ✓ Deshifrlash va tekshirish. Agar deshifrlash imkoni bo‘lmasa (nostandart kripto-algoritm, eskirgan sertifikat va boshqa holatlar) – taqiqlash;
15. Ma’lum URL kategoriyalari va alohida ishonchli veb-saytlarni deshifrlamaslik;
16. Ilovalar, IP-manzillar, foydalanuvchilar va foydalanuvchi guruhlari asosida QoS siyosatlari yordamida DSCP belgilash va trafikni cheklash;
17. Ilova darajasida aniqlangan real-time trafik uchun apparat QoS realizatsiyasi;
18. Siyosatga asoslangan trafik yo‘naltirishni (Policy Based Forwarding) qo‘llash;
19. Ilovaning alohida funksiyalariga ruxsat berish;
20. Yuqorida sanab o‘tilgan amallarning istalgan kombinatsiyasi.
21. Antivirus himoyasi, spyware dan himoya, zaifliklar va tarmoq hujumlariga qarshi himoya (hujumlarni aniqlash va oldini olish tizimi), dinamik obro‘ bazasidan foydalangan URL-filtrlash, bir xil veb-saytning turli bo‘limlari uchun kategoriyalarni qo‘llab-quvvatlash, jumladan rus tilidagi veb-saytlar uchun kategoriyalar, fayllarni turiga qarab bloklash, ma‘lum signaturalar bo‘yicha;
22. Internet tarmog‘i resurslariga bo‘lgan so‘rovlarni resurs kategoriyasiga qarab aniqlash va filtrdan o‘tkazish, masalan zararli saytlar, ijtimoiy tarmoqlar, reklama resurslari va h.k.;
23. Quyidagi amallarni qo‘llab-quvvatlash: ruxsat berish, xabar berish, bloklash, foydalanuvchidan tasdiq so‘rash, foydalanuvchi parolini so‘rash;
24. URL-filtrlash tahdidlarga javob berish vaqtini kamaytirish uchun mashinali o‘qitish texnologiyasidan foydalanib amalga oshirilishi kerak;
25. SNIcat turidagi aylanib o‘tish texnikalariga qarshi turish maqsadida TLS Hello da SNI va HTTP so‘rovidagi URL ni bir vaqtda tahlil qilish;
26. Shubhali DNS-so‘rovlarni, DGA domenlarini tahlil qilish va DNS sinkhole texnologiyasi yordamida yuqtirilgan stansiyalarni aniqlash (DNS-server javobini almashtirish);
27. DNS-so‘rovlardan foydalangan holda himoya vositalarini aylanib o‘tish texnikalarini aniqlash, jumladan mashina tomonidan yaratilgan DGA domen nomlari, n-gram chastota tahlili, entropiya tahlili, so‘rov chastotasi, DNS ichida tunnellash, DNS-so‘rovlar orqali ma’lumot uzatish kanallari, shu jumladan juda sekin DNS-tunnellar;

28. DGA domenlarini, lug‘at asosida yaratilgan DGA domenlarini, DNS-rebinding aylanma texnikalarini, FastFlux, Dangling DNS yozuvlariga murojaatlarni, NSNX hujumlarini, yaqinda ro‘yxatdan o‘tgan domenlarga hujumlarni bloklash;
29. Shubhali DNS-so‘rovlarni tahlil qilish tahdidlarga javob berish vaqtini kamaytirish uchun mashinali o‘qitish texnologiyasidan foydalanib amalga oshirilishi kerak;
30. Aylanib o‘tish (evasions) texnikalaridan himoya, masalan MPTCP;
31. Potensial zararli noma’lum fayllarni sandbox muhitida skanerlash xizmatini taqdim etish, Microsoft Windows va Linux operatsion tizimlarida faylni ishga tushirish va hujjatlarni ko‘rish metodlari orqali;
32. Sandbox shubhali bajariladigan fayllarni (jumladan EXE, DLL, SCR, BAT va boshqalar), ELF fayllar, PDF formatidagi hujjatlar, MS Office 2003, 2007 va undan yuqori, Java va Flash, Android APK, Mach-O, DMG va PKG fayllari, RAR, ZIP, 7Zip arxivlari tekshirishi kerak;
33. Tarmoqlararo ekran HTTP, HTTPS, SMTP, POP3, IMAP, SMB, FTP ilovalarida uzatiladigan shubhali fayllarni sandbox ga tekshirish uchun yuborishi kerak, shuningdek mavjud bo‘lsa, SSL orqali uzatilgan fayllarni ham;
34. Sandbox fayl tekshiruvi bo‘yicha hisobot yaratishi va tarmoqlararo ekranga yuborishi kerak;
35. Sandbox zero-day bloklash uchun signaturalar yaratishi va fayl tekshiruvidan so‘ng 5 daqiqa ichida kompaniyaning barcha tarmoqlararo ekranlarida sanab o‘tilgan ilovalarda ishlatish uchun yuborishi kerak;
36. Tarmoqlararo ekran sandboxdan fayl signaturalarini olishi va bulutli yoki mahalliy sandboxdan olingan yangi signaturalar bo‘yicha bloklash mexanizmiga ega bo‘lishi kerak;
37. Yetkazib beruvchi bulutli sandbox barcha mijozlar o‘rtasida signaturalarni almashish imkoniyatiga ega bo‘lishi kerak;
38. Tarmoqlararo ekran sandbox dan kompрometatsiya indikatorlarini olishi kerak: IP, URL, DNS, zararli kod tomonidan ishlatiladigan va zararli indikatorlar ro‘yxati bo‘yicha ulanishlarni bloklash;
39. Sandbox SMTP/POP3 protokollari orqali elektron pochtadagi http:// va https:// havolalarni tekshirishi kerak;
40. Sandbox SSL bilan shifrlangan ilovalardagi fayllarni, kamida HTTPS protokoli bo‘yicha tekshirishi kerak;
41. Nolinchi kun tahdidlarini inspeksiya qilishda mashinali o‘qitishni qo‘llab-quvvatlash majburiy bo‘lib, shubhali faylni tekshirishdagi kechikishni kamaytiradi;
42. Sandbox shubhali fayllar va havolalarning xulq-atvorini shaxsiy yoki tashqi bulutda (“sandbox”) tahlil qilishi, yangi zararli dasturlarni aniqlashi, 5 daqiqa ichida avtomatik antivirus siganturasini yaratishi va 30 daqiqa ichida URL reputatsiya bazasini yangilashi, va bu barcha mijoz qurilmalariga tegishli obunalar bilan o‘rnatilishi kerak;
43. Nolinchi kun tahdidlarini aniqlash subsistemasi bilan integratsiya imkoniyati: bu subsistema bir xil yetkazib beruvchining maxsus apparat qurilmasi asosida markaziy mijoz ob’ektida (xususiy bulut) joylashtiriladi va mijozning ma’lumotlarni qayta ishlash markazidagi ajratilgan apparat qurilmasida 5 daqiqa ichida antivirus signaturasini avtomatik yaratishga imkon beradi;
44. Ajratilgan mahalliy sandbox API ga ega bo‘lishi kerak, fayllarni tekshirish uchun tarmoqlararo ekrandan qabul qilish imkoniyati bilan;
45. Sandbox bajarilgan tekshiruvlar bo‘yicha hisobotlar yaratishi va ushbu hisobotlarni PDF formatida ko‘rish imkoniyatiga ega bo‘lishi kerak;

46. Bulutli sandbox operatsion tizim emulyatsiyasini ishlatmasdan Bare metal analysis texnologiyasini qo‘llashi kerak;
47. Tarmoqlararo ekran turli fayl turlarini turli sandboxlarga yuborish imkoniyatiga ega bo‘lishi kerak, masalan exe fayllar bulutli sandboxga, DOC fayllar esa mahalliy sandboxga;
48. Bulutli sandbox PE (Portable Executable) fayllarni tekshirish uchun qabul qilishi kerak, obuna mavjud bo‘lmasa ham;
49. Rivojlangan vizualizatsiya funksiyalari: tarmoq ilovalari faoliyati, aniqlangan va bloklangan tarmoq tahdidlarini oddiy va qulay o‘qiladigan formatda vizualizatsiya qilish; ma’lumotni turli filtrlar orqali filtrlash imkoniyati (ilovalar, tahdidlar, foydalanuvchilar, IP-manzillar, TCP/UDP portlar, xavfsizlik zonalari, tahdid turlari va boshqalar);
50. Avtomatik loglar korrelyatsiyasi**:** turli turdagi loglarni (tarmoqlararo ekran, tahdidlardan himoya, fayl uzatishni nazorat qilish, URL-filtrlash) bitta seans doirasida avtomatik bog‘lash;
51. Tarmoqlararo ekranda axborot xavfsizligi voqealarini avtomatik korrelyatsiya qilish imkoniyati, yangilanadigan korrelyatsiya ob’yektlari orqali amalga oshiriladi, bu ob’yektlar antivirus himoyasi, spyware dan himoya, zaifliklar va tarmoq hujumlaridan himoya, nolinchi kun tahdidlardan himoya bo‘yicha va korrelyatsiya ob’yekti ishga tushgan foydalanuvchi uchun ikki faktorli autentifikatsiya (MFA - ko‘p omilli autentifikatsiya) orqali majburiy autentifikatsiya imkoniyatini beruvchi ishchi stansiyalardan olingan ma’lumotlarni ishlatishi kerak;
52. Quyidagi Multi-Factor Authentication (MFA) provayderlarini qo‘llab-quvvatlash (to‘g‘ridan-to‘g‘ri, oraliq mahsulotlarsiz): Duo, Okta, RSA SecureID, PingID;
53. AD bilan integratsiya orqali foydalanuvchi login va parollarini o‘g‘irlashdan himoya, hisob qaydlarini ishonchsiz xavfsizlik zonasiga uzatilishini monitoring qilish, ikki faktorli autentifikatsiya (MFA) orqali majburiy autentifikatsiya;
54. DoS hujumlaridan himoya funksiyasi mavjudligi;
55. ICMP/TCP/UDP port skanerlashini bloklash funksiyasi mavjudligi;
56. Tarmoq orqali uzatiladigan fayllarda muhim ma’lumotlarni o‘z ichiga olgan obyektlarni aniqlash va bunday fayllarni uzatishni bloklash;
57. Tarmoq orqali uzatiladigan fayllarda filtrlanadigan ma’lumotlarni aniqlash, jumladan, lekin cheklanmagan holda: Adobe PDF, HTML, Microsoft Office (Excel, Word, PowerPoint), Rich Text Format;
58. Oldindan sozlangan ma’lumot shablonlari mavjudligi, masalan, kredit kartalarining raqamlari;
59. O‘z shablonlarini yaratishni qo‘llab-quvvatlash, muntazam ifodalar asosida;
60. Hisobotlar yaratish: tarmoqlararo ekran avtomatik va reja bo‘yicha turli mavzularda (aniqlangan tahdidlar, foydalanuvchilar va ilovalar bo‘yicha uzatilgan ma’lumot hajmi va boshqa) hisobotlar yaratish funksiyalariga ega bo‘lishi kerak; qo‘lda hisobotlarni sozlash imkoniyati; hisobotlarni to‘g‘ridan-to‘g‘ri grafik web interfeysi (GUI) orqali ko‘rish va PDF hamda CSV formatlariga eksport qilish imkoniyati.
61. Bir xil yetkazib beruvchi tarmoqlararo ekranlarining markazlashtirilgan boshqaruv, loglash, hisobot va dasturiy ta’minot yangilash subsistemasi bilan integratsiya qilish;
62. Deshifrlangan SSL trafigini tashqi qurilmalarga yuborish funksiyasining mavjudligi;
63. Tashqi qurilmalardan trafikni olish va uni Internet orqali uzatish uchun SSL tunelida shifrlash funksiyasi;
64. Markazlashtirilgan loglash subsistemasi qisqa muddatga mavjud bo‘lmaganda, loglarni mahalliy ichki qattiq diskda buferlash;
65. SaaS turidagi ilovalar bo‘yicha alohida hisobot mavjudligi;

66. IPSec VPN, SSL VPN va clientless VPN SSL funksiyalarining mavjudligi;
67. Korporativ ish muhiti uchun masofaviy foydalanuvchilarni, foydalanuvchi ish stansiyasida ma’lum dasturlar mavjudligini tekshirish imkoniyati bilan granulyar nazorat qilish,.
68. Syslog protokoli orqali uchinchi tomon SIEM/SIM tizimlari bilan integratsiya, log formatini moslashuvchan sozlash imkoniyati bilan;
69. Mahalliy administratorlar uchun rol asosida kirish boshqaruvi:
    - ✓ Qurilmaning umumiy darajasida ham, alohida virtual tizimlar (kontekstlar) darajasida ham ko‘rish va boshqarish hududini cheklash imkoniyati;
    - ✓ NGFW web-interfeysining har qanday bo‘limiga tahrirlash yoki faqat o‘qish rejimida kirish berish, yoki kirishni butunlay taqiqlash imkoniyati;
    - ✓ NGFW CLI ga tahrirlash yoki faqat o‘qish rejimida kirish berish, yoki kirishni butunlay taqiqlash imkoniyati..
70. Apparatli tarmoqlararo ekran maxsus apparat platformasiga ega bo‘lishi kerak, bu qurilma to‘liq yuklangan holatda ham boshqarishni to‘xtatmasdan amalga oshirish imkonini beradi. Nazorat qilinadigan trafikni qayta ishlash uchun va boshqaruv vazifalarini bajarish uchun alohida hisoblash resurslari ta’minlanishi lozim;
71. Har bir alohida qurilmani boshqarish HTTPS va SSH protokollari orqali amalga oshirilishi kerak, administrator ish stansiyasida qo‘shimcha boshqaruv dasturini o‘rnatish shart bo’lmasligi kerak;
72. Taklif etilayotgan tarmoqlararo ekran “Internet of Things” (IoT) qurilmalarni aniqlashni qo‘llab-quvvatlashi kerak;
73. Taklif etilayotgan tarmoqlararo ekran, kvantga chidamli kriptografiya (Quantum-Resistant Cryptography) dan foydalanish imkoniyati bilan, kvant hisoblash hujumlaridan himoyalangan algoritmlarga asoslangan, RFC 8784, RFC 9242, RFC 9370 standartlariga muvofiq IPsec-tunnellarni qo‘llab-quvvatlashi kerak;
74. Taklif etilayotgan tarmoqlararo ekran DNS hijacking (DNS so‘rov yoki javob marshrutining o‘zgarishi natijasida IP-manzillarning almashtirilishi) turidagi hujumlarni aniqlash va oldini olish imkoniyatiga ega bo‘lishi kerak.
75. Taklif etilayotgan tarmoqlararo ekran tarmoqdagi qurilmalarni ko‘plab xususiyatlar, jumladan: MAC-manzil, IP-manzil, operatsion tizim, qurilma turi va boshqa parametrlar bo‘yicha aniqlashni qo‘llab-quvvatlashi va ushbu ma’lumotlar asosida axborot xavfsizligi siyosatlarini qo‘llash imkoniyati bo’lishi kerak.
76. Tarmoqlararo ekran boshqaruv interfeysi (veb va CLI) markazlashtirilgan boshqaruv, loglash, hisobot va dasturiy ta’minotni yangilash subsistemasi bilan birxillashtirilgan bo‘lishi kerak;
77. Markazlashtirilgan boshqaruv, loglash, hisobot va dasturiy ta’minotni yangilash tizimi mijozning mavjud serverlarida ishga tushirilishi kerak.
78. Taklif etilayotgan tarmoqlararo ekran URLlarni tahlil qilish va filtrlashni ta’minlashi, shu jumladan veb-sahifalardagi zararli JavaScriptlarni aniqlash imkoniyatiga ega bo‘lishi kerak.
79. Taklif etilayotgan tarmoqlararo ekran avtomatik tahlildan qochish uchun CAPTCHA ishlatadigan zararli va fishing veb-sahifalarni aniqlash va bloklashni ta’minlashi kerak.
80. Taklif etilayotgan tarmoqlararo ekran 41 tilda skanerlash va tahlil qilishni qo‘llab-quvvatlashi kerak.
81. Tarmoqlararo ekran Perfect Forward Secrecy (PFS) ta’minlaydigan kriptografik algoritmlar va shifrlash to‘plamlaridan foydalanish imkoniyatini ruxsat berish yoki cheklashni xavfsizlik siyosatlariga muvofiq ta’minlashi kerak.

82. Xarid qilinayotgan uskunalar Mijoz tomonidan tarmoq perimetri xavfsizligini markazlashtirilgan boshqarish va nazorat qilish uchun ishlatiladigan Panorama tizimi bilan mos bo‘lishi kerak.

6.2. NGFW uskunasiga qo‘yiladigan talablar

№ va pozitsiya nomi	Pozitsiya ta'rifi va talablar	Soni
1. Yirik va kichik filiallar uchun tarmoqlararo ekranlar (1-tur)	**Minimal umumiy talablar:** • 10/100/1000 Mbit Ethernet RJ-45 porti – kamida 8 ta; • RJ-45 ulagichli 10/100/1000 Mbit Ethernet tarmoqlararo ekranni boshqarish uchun ajratilgan (tarmoqdan tashqari) port – kamida 1 ta port; • RJ-45 ulagichiga ega konsolli boshqaruv porti - kamida bitta; • Micro-USB ulagichiga ega konsol boshqaruv porti - kamida bitta; • Ishlab chiqaruvchi tomonidan e’lon qilingan har bir qurilmaning tarmoqlararo ekranlash rejimidagi ilovalarni identifikatsiyalashni ta’minlagan holda o‘tkazuvchanlik qobiliyati – kamida 1.8 Gbit/s; • Ishlab chiqaruvchi tomonidan e’lon qilingan qurilmaning tarmoqlararo ekranlash rejimidagi o‘tkazish qobiliyati, ilovalarni identifikatsiya qilish, bir vaqtning o‘zida ilova darajasidagi (Layer 7) trafikni tahlil qilish, zaiflik signaturalarining to‘liq to‘plamidan foydalangan holda hujumlarning oldini olish, zararli dasturiy ta’minot va josuslik dasturlaridan himoya qilish, uzatilayotgan fayllarni tekshirish va nazorat qilish, noma’lum tahdidlar mavjudligini aniqlash uchun fayllarni ilg‘or tahlil qilishni ta’minlagan holda, shuningdek, xavfsizlik jurnallarini yuritish funksiyalarini yoqish bilan – kamida 1,2 Gbit/s; • 64 kB tranzaksiya uzunligidagi HTTP trafigida, ishlatiladigan TCP/UDP portidan qat’i nazar, OSI modelining 7-darajasidagi ilovalarni aniqlash funksiyasi yoqilganda o‘lchanadigan IPsec VPN o‘tkazish qobiliyati – kamida 0,8 Gbit/sek; • Ilovalar darajasidagi bir vaqtning o‘zida qo‘llab-quvvatladigan seanslar soni - kamida	**22 dona.**

	98 000 ta; - Ilovalar darajasidagi qo‘llab-quvvatladigan yangi seanslar soni sekundiga – kamida 15 000 ta; - Xotira hajmi - 128 GB **Minimal funksional talablar:** - IKEv1, IKEv2 (PSK va sertifikat asosida) - Shifrlash: 3DES, AES (128/192/256-bit) - Autentifikatsiya: MD5, SHA-1, SHA-256, SHA-384, SHA-512 - Bitta qurilma/interfeys uchun 4094 tagacha VLAN 802.1q tegini qo‘llab-quvvatlash - Interfeyslarini birlashtirish 802.3ad LACP - NAT (IPv4) rejimlari: statik IP, dinamik IP, dinamik IP va port (port manzilini o‘zgartirish), - NAT64, NPTv6 - NATning qo‘shimcha funksiyalari: IP-manzillarni dinamik zaxiralash, sozlanadigan dinamik IP-manzil va portlarga qayta obuna bo‘lish. - Statik marshrutlash va dinamik marshrutlash(MP-BGP kengaytmalari va Graceful Restart mexanizmlari bilan BGP, OSPFv2/v3, RIP) protokollarini qo‘llab-quvvatlash - IPv4 va IPv6 manzillarini dinamik belgilash bilan PPPoE-mijoz rejimida ishlash; - Multicast qo‘llab-quvvatlash - PIM-SM, PIM-SSM, IGMP v2/v3. **Nosozlikka chidamlilik funksiyalari:** - Rejimlar: aktiv/aktiv, aktiv/passiv, HA (High Availability) klasterlash - Nosozliklarni aniqlash: yo‘l (path) monitoringi, interfeys monitoringi **Komplektatsiyaga qo‘yiladigan talablar:** - Tashqi elektr ta’minoti moduli, quvvati kamida 40 Vt, kirish kuchlanishi 100–240 VAC (50–60 Hz). - Har bir elektr ta’minoti bloki uchun Euro Plug turidagi quvvat shnurlari. **Minimal kafolat va litsenziya talablari:** - Yetkazib beriladigan barcha uskunalar va dasturiy ta’minot uchun kafolat muddati kamida 12 oy; - Qurilma ishlab chiqaruvchi tomonidan kamida 12 oy muddatga texnik qo‘llab-quvvatlash,	

	uskuna ishdan chiqqan taqdirda uni oldindan almashtirish;
	- Yetkazib berish tarkibiga amal qilish muddati kamida 12 oy bo‘lgan quyidagi litsenziyalar kiritilgan bo‘lishi kerak:
	  - DNS tahdidlardan ilg‘or himoya;
	  - Noma’lum tahdidlarni tahlil qilish uchun bulutli sandbox;
	  - Takomillashtirilgan URL filtrlash himoyasi;
	  - Takomillashtirilgan tahdidlarni oldini olish tizimi;
	  - Takomillashtirilgan SD-WAN;
	  - Tarmoq qurilmalarini (IoT) aniqlash va himoya qilish.	

2. 1-tur Tarmoqlararo ekran uskunasi uchun "sovuq zaxira" (Cold Spare)	**Minimal umumiy talablar:** - 10/100/1000 Mbit Ethernet RJ-45 porti – kamida 8 ta; - RJ-45 ulagichli 10/100/1000 Mbit Ethernet tarmoqlararo ekranni boshqarish uchun ajratilgan (tarmoqdan tashqari) port – kamida 1 ta port; - RJ-45 ulagichiga ega konsolli boshqaruv porti - kamida bitta; - Micro-USB ulagichiga ega konsol boshqaruv porti - kamida bitta; - Ishlab chiqaruvchi tomonidan e’lon qilingan har bir qurilmaning tarmoqlararo ekranlash rejimidagi ilovalarni identifikatsiyalashni ta’minlagan holda o‘tkazuvchanlik qobiliyati – kamida 1.8 Gbit/s; - Ishlab chiqaruvchi tomonidan e’lon qilingan qurilmaning tarmoqlararo ekranlash rejimidagi o‘tkazish qobiliyati, ilovalarni identifikatsiya qilish, bir vaqtning o‘zida ilova darajasidagi (Layer 7) trafikni tahlil qilish, zaiflik signaturalarining to‘liq to‘plamidan foydalangan holda hujumlarning oldini olish, zararli dasturiy ta’minot va josuslik dasturlaridan himoya qilish, uzatilayotgan fayllarni tekshirish va nazorat qilish, noma’lum tahdidlar mavjudligini aniqlash uchun fayllarni ilg‘or tahlil qilishni ta’minlagan holda, shuningdek, xavfsizlik jurnallarini yuritish funksiyalarini yoqish bilan – kamida 1,2 Gbit/s; - 64 kB tranzaksiya uzunligidagi HTTP	**3 dona.**

	trafigida, ishlatiladigan TCP/UDP portidan qat'i nazar, OSI modelining 7-darajasidagi ilovalarni aniqlash funksiyasi yoqilganda o'lchanadigan IPsec VPN o'tkazish qobiliyati – kamida 0,8 Gbit/sek; • Ilovalar darajasidagi bir vaqtning o'zida qo'llab-quvvatladigan seanslar soni - kamida 98 000 ta; • Ilovalar darajasidagi qo'llab-quvvatladigan yangi seanslar soni sekundiga – kamida 15 000 ta; • Xotira hajmi - 128 GB **Minimal funksional talablar:** • IKEv1, IKEv2 (PSK va sertifikat asosida) • Shifrlash: 3DES, AES (128/192/256-bit) • Autentifikatsiya: MD5, SHA-1, SHA-256, SHA-384, SHA-512 • Bitta qurilma/interfeys uchun 4094 tagacha VLAN 802.1q tegini qo'llab-quvvatlash • Interfeyslarini birlashtirish 802.3ad LACP • NAT (IPv4) rejimlari: statik IP, dinamik IP, dinamik IP va port (port manzilini o'zgartirish), • NAT64, NPTv6 • NATning qo'shimcha funksiyalari: IP-manzillarni dinamik zaxiralash, sozlanadigan dinamik IP-manzil va portlarga qayta obuna bo'lish. • Statik marshrutlash va dinamik marshrutlash(MP-BGP kengaytmalari va Graceful Restart mexanizmlari bilan BGP, OSPFv2/v3, RIP) protokollarini qo'llab-quvvatlash • IPv4 va IPv6 manzillarini dinamik belgilash bilan PPPoE-mijoz rejimida ishlash; • Multicast qo'llab-quvvatlash - PIM-SM, PIM-SSM, IGMP v2/v3. **Nosozlikka chidamlilik funksiyalari:** • Rejimlar: aktiv/aktiv, aktiv/passiv, HA (High Availability) klasterlash • Nosozliklarni aniqlash: yo'l (path) monitoringi, interfeys monitoringi	
3. 1-tur Tarmoqlararo ekran uskunasi uchun qo'shimcha quvvat bloklari	• Tashqi elektr ta'minoti moduli, yetkazib beriladigan uskuna (TE, 1-tur) bilan to'liq mos bo'lishi kerak; • Quvvati kamida 40 Vt, kirish kuchlanishi 100–240 VAC (50–60 Hz); • Har bir elektr ta'minoti bloki uchun Euro Plug turidagi quvvat shnurlari.	**5 dona**

8. Obunalarni uzaytirish va texnik qo‘llab-quvvatlashga qo‘yiladigan talablar

№ va pozitsiya nomi	Litsenziyalar tavsifi va ularga qo‘yiladigan talablar	Soni
1. Palo Alto PA-3260 uchun obunalarni (litsenziyalarni) uzaytirish	**Amal qilish muddati 12 oydan kam bo’lmagan quyidagi litsenziya va xizmatlar to‘plamini yetkazib berish hamda faollashtirish:** • Advanced Threat Prevention • Advanced URL Filtering • Advanced WildFire • Advanced DNS Security • Advanced SD-WAN • Device Security • Premium Support	**4 dona**
2. Palo Alto PA-3430 uchun obunalarni (litsenziyalarni) uzaytirish	**Amal qilish muddati 12 oydan kam bo’lmagan quyidagi litsenziya va xizmatlar to‘plamini yetkazib berish hamda faollashtirish:** • Advanced Threat Prevention • Advanced URL Filtering • Advanced WildFire • Advanced DNS Security • Advanced SD-WAN • Prisma Access Agent • Device Security • Premium Support.	**2 dona.**
3. Palo Alto PA-410 uchun obunalarni (litsenziyalarni) uzaytirish	**Amal qilish muddati 12 oydan kam bo’lmagan quyidagi litsenziya va xizmatlar to‘plamini yetkazib berish hamda faollashtirish:** • Advanced Threat Prevention • Advanced URL Filtering • Advanced WildFire • Advanced DNS Security • Advanced SD-WAN • Device Security • Premium Support	**43 dona.**

9. Butlovchi qismlar va boshqaruv tizimining litsenziyalarini yangilash bo‘yicha talablar

№ va pozitsiya nomi	Texnik talablar va tavsif	Soni
4. Amaldagi Palo Alto PA-410 uchun zaxira quvvat bloki	• Tashqi quvvat moduli, quvvati kamida 25 Vt, kirish kuchlanishi 100–240 VAC (50–60 Hz). • Har bir quvvat bloki uchun Euro Plug quvvat simlari bilan jamlangan holda.	**5 dona**

5. Amaldagi VM Panorama uchun litsenziya	Panorama (Virtual Appliance) markazlashtirilgan boshqaruv tizimi uchun litsenziyani uzaytirish va kengaytirish. Litsenziyaning funksional hajmi quyidagilarni ta’minlashi kerak: • 1000 tagacha qurilmalarni boshqarishni (Device Management) faollashtirish; • Kamida 12 oy muddatga texnik qo‘llab-quvvatlash (Support).	**1 dona**

10. Ijrochi qo‘yiladigan talablar

Ijrochi quyidagi malaka talablariga javob berishi lozim:

1. Axborot texnologiyalari va/yoki telekommunikatsiya infratuzilmasini yetkazib berish sohasida kamida 2 yillik rasmiy tajribaga ega bo'lishi — mazkur loyiha doirasida amalga oshirilayotganlarga kapital qo'yilmalar hajmi va/yoki tizimlar ro'yxati jihatidan o'xshash bo'lgan loyihalar tajribasi imzolangan shartnomalar yoki hisob-fakturalar bilan tasdiqlanishi lozim;
2. Taklif etilayotgan yechim ishlab chiqaruvchisi bo'yicha sertifikatlangan muhandislarga ega bo'lishi (kamida 1 ta sertifikat);
3. Ijrochi zaruriy vakolatlandirish maqomlariga ega bo'lishi va ushbu TT bo'yicha talab qilingan yetkazib berishni to'liq hajmda amalga oshirish uchun barcha uskuna, dasturiy ta'minot va materiallar ishlab chiqaruvchilaridan vakolatlandirish xatlarini (Manufacturer Authorization Letter) taqdim etishi lozim.

11. Texnik ishlar ro‘yxati (Palo Alto Networks)

Ushbu bo‘lim Palo Alto Networks uskunalari bo‘yicha amalga oshiriladigan texnik ishlarning to‘liq ro‘yxatini o‘z ichiga oladi va ushbu Texnik Topshiriqning ajralmas qismi hisoblanadi.

10.1 Loyihalash

Texnik ishlar boshlanishidan oldin Ijrochi ikkita loyiha hujjatini ishlab chiqadi va ularni Buyurtmachi bilan tasdiqlaydi. Hujjatlar imzolanmagan holda uskunani ishga tushirishga yo‘l qo‘yilmaydi.

Kontseptual loyiha (KL) qarorning umumiy arxitekturasini ifodalaydi: tarmoqni taqsimlash mantig‘i, filiallarni birlashtirish sxemasi, kanallarni zaxiralash va trafikni markazlashtirilgan nazorat qilish tamoyillari. Hujjat texnik mutaxassislar uchun ham, buyurtmachi rahbariyati uchun ham tushunarli bo‘lishi kerak.

Ishchi loyiha (IL) muayyan sozlash parametrlarini o‘z ichiga oladi: manzil maydoni, xavfsizlik siyosati konfiguratsiyasi, SD-WAN sozlamalari, markazlashtirilgan boshqaruv tizimi namunalari, loglarni uzatish sozlamalari va SSL tekshiruvi. Hujjat kelgusidagi barcha ishlarni amalga oshirishda asos bo‘ladi.

10.2. Markazlashtirilgan boshqaruv tizimi (Panorama) ni isloh qilish

Palo Alto Panorama — barcha tarmoqlararo ekranlar parkini markazlashgan holda boshqarish tizimi. Hozirgi holatda barcha 43 ta filial qo‘lda bajariladigan yagona shablon orqali boshqariladi, bu esa xizmat ko‘rsatishni qiyinlashtiradi va xatolar xavfini oshiradi.

Ijrochi amaldagi konfiguratsiya auditini o‘tkazadi va boshqaruv tizimini qayta quradi: qurilmalar turi va joylashuvi bo‘yicha mantiqiy guruhlarga ajratiladi (MQM, bosh ofis, yirik va kichik filiallar) har bir guruh uchun alohida sozlash shablonlari yaratiladi. Zarurat tug‘ilganda, Panoramaning yangi nusxasi kengaytirilib, konfiguratsiya o‘tkaziladi.

10.3. Yangi tarmoqlararo ekranlarni (Yirik va kichik filiallar uchun tarmoqlararo ekranlar (1-tur)) o‘rnatish va dastlabki sozlash

Sotib olinadigan 22 ta yirik va kichik filiallar uchun tarmoqlararo ekranlar (1-tur) qurilmasi bank filiallariga foydalanishga topshiriladi. Ushbu qurilmalari joylashtirilishi natijasida almashtirilgan PA-410 qurilmalari boshqa kichik filiallarga o’rnatib, sozlash ishlari yetkazib beruvchi tomonidan amalga oshiriladi. Bo‘shatilgan PA-410 qurilmalarini kichik filiallarga jismonan ko‘chirish Buyurtmachi tomonidan amalga oshiriladi.

Uskunalarni hududlar bo‘ylab tashish va qurilmalarni tayanchlarga o‘rnatish ishlari Buyurtmachi tomonidan amalga oshiriladi. Sozlash bo‘yicha barcha ishlar Ijrochi tomonidan Panorama orqali masofadan turib amalga oshiriladi va quyidagilarni o‘z ichiga oladi: qurilmani boshqaruv tizimida ro‘yxatdan o‘tkazish, litsenziyalarni faollashtirish, operatsion tizimni tavsiya etilgan eng so‘nggi versiyaga yangilash, siyosat shablonlarini joriy etish.

10.4. SD-WAN sozlash

Ijrochi barcha 61 ta filialda (43 ta amaldagi va 18 ta yangi) tarmoqlararo ekranlarda SD-WAN ni sozlaydi. Siyosatlar ishchi loyiha doirasida (10.1-band) ishlab chiqiladi va Panorama orqali markazlashtirilgan holda qo‘llaniladi. Sozlamalar filiallardagi legacy uskunalardan yangi **Yirik va kichik filiallar uchun tarmoqlararo ekranlar (1-tur)** qurilmalariga ko‘chiriladi.

10.5. Loglarni markazlashtirish va SIEM tizimi bilan integratsiya

Tarmoqlararo ekranlar barcha xavfsizlik hodisalarini qayd etadi: ulanishlar, siyosat ishga tushishlari, aniqlangan tahdidlar. Ushbu ma‘lumotlar axborot xavfsizligi xizmati tomonidan SIEM tizimida (QRadar) monitoring uchun foydalaniladi.

Ijrochi ikki bosqichli sxemani sozlaydi: barcha qurilmalar (MQM, bosh ofis, barcha filiallar) loglarni Panorama ga uzatadi, Panorama esa ularni markazlashtirilgan va tanlab QRadar ga yuboradi. Bu yagona nuqtada ma‘lumotlar oqimlarini boshqarish va SIEM litsenziyalarini ortiqcha sarflamaslik imkonini beradi.

10.6. SSL-inspeksiyani sozlash

Ijrochi PA-3260 da SSL-inspeksiyani sozlaydi. SSL-inspeksiya qurilmaga trafikni shifrlash, tekshirish va qayta shifrlash imkonini beradi — foydalanuvchi uchun shaffof tarzda. Sozlash jarayonida tekshirilishi kerak bo‘lgan trafik toifalari va istisnolar belgilanadi.

10.7. User-ID sozlamalari

Ijrochi infratuzilmaning kengayishini va Buyurtmachi muhitining xususiyatlarini hisobga olgan holda User-ID sozlamasini amalga oshiradi va mavjud konfiguratsiyani yangilaydi, jumladan bir necha xodim bir vaqtning o‘zida bitta IP-manzil ostida ishlaydigan terminal serverlarda foydalanuvchilarni to‘g‘ri identifikatsiya qilishni ta‘minlaydi.

10.8. Filial tarmog‘ini migratsiya qilish

65 ta filialda uskunalarni almashtirish ishlari Buyurtmachi bilan kelishilgan jadvalga muvofiq bosqichma-bosqich amalga oshirilmoqda. Har bir filialni yangi uskunalarga o‘tkazish oldindan belgilangan servis vaqtida, odatda, ishdan tashqari paytda bajariladi.

Barcha xizmatlarning mavjudligi, SD-WANning to‘g‘ri ishlashi, loglarning Panorama’ga uzatilishi va foydalanuvchilarning to‘g‘ri identifikatsiyasi tasdiqlangandan so‘ng, o‘tish jarayoni yakunlangan deb hisoblanadi.

kelishuvchilar: B.Shamsiev, Z.Orifkhojayev

https://hujjat.brb.uz/?pin=sI53lT37&id=5c59edd4-f4db-45a4-883d-3292cfa700cb