Հավելված 1

1. Ներածություն

1.1 Նպատակ

ԱՄԻՕ Բանկ ՓԲԸ հրավիրում է որակավորված մատակարարներին ներկայացնել առաջարկներ Ethernet VPN (EVPN) Fabric, ձեռնարկության firewall-ներ և կենտրոնացված կառավարման համակարգեր կառուցելու համար անհրաժեշտ ցանցային սարքավորումների մատակարարման վերաբերյալ: Առաջարկվող լուծումները պետք է ապահովեն բարձր արդյունավետություն, մասշտաբայնություն և կայուն տվյալների կենտրոնի ցանցային կապ, որը հնարավորություն կտա անխափան երթուղայնացում, կամուրջների ստեղծում և ինտեգրում վիրտուալ հարթակներում: Ընտրված բոլոր սարքավորումները պետք է համապատասխանեն խիստ տեխնիկական պահանջներին՝ ցածր լատենտությամբ գործողություններ, հուսալի անվտանգություն և արդյունավետ կառավարում ապահովելու համար:

1.2 Նախապատմություն

AMIO Բանկը իրականացնում է իր տվյալների կենտրոնի ենթակառուցվածքների արդիականացման նախագիծ: EVPN Fabric-ը կկազմի այս արդիականացման հիմքը՝ հնարավորություն տալով ունենալ վիրտուալացված աշխատանքային բեռներ, բազմավարձակալություն և բարձր արագության կապ: Առաջարկները պետք է լիարժեք համապատասխանեն այս փաստաթղթում նշված պահանջներին և առաջարկեն ծախսարդյունավետ, փոխգործունակ և կայուն լուծումներ:

1.3 Նպատակներ

- Ձեռք բերել spine, leaf, service leaf/DCI սարքեր, որոնք աջակցում են EVPN/VXLAN-ին երթուղայնացման և կամուրջների ստեղծմանը:
- Ձեռք բերել բարձակարգ Firewall-ներ սահմանային, տվյալների կենտրոնի, Zero Trust Network Access Firewall (ZTNA) / User Access GW և WAN միջավայրերի համար:
- Ներառել բոլոր անհրաժեշտ օպտիկական փոխանցող-հաղորդիչները (SFP/SFP+/SFP28/QSFP+) և կառուցվածքային մալուխները:
- Համոզվել, որ սարքավորումները համապատասխանում են կատարողականի, հուսալիության և մասշտաբայնության պահանջներին:
- Հեշտացրել ցանցի և անվտանգության ինտեգրացիան՝ VMware NSX-ի և Nutanix Flow-ի նման ծրագրային ծածկույթների միջոցով:
- Առաջնահերթություն տալ այն մատակարարներին, որոնք առաջարկում են համապարփակ մոնիթորինգի, սպասարկման և հեռաչափման հնարավորություններ:

2. Աշխատանքի շրջանակը

Վաճառողները պարտավոր են տրամադրել իրենց համապատասխան լուծումները: Աշխատանքների շրջանակը ներառում է.

- **Ցանցային սարքավորումներ.** Spine, leaf և service leaf/DCI կոմուտատորներ, որոնք համապատասխանում են նշված միացքների կոնֆիգուրացիա, բուֆերի չափերին և փոխանցման հզորություններին, ինչպես նաև հնարավորություններ EVPN Fabric տեղակայման համար, ներառյալ երթուղայնացումը, QoS-ը, անվտանգությունը և հեռաչափությունը:
- **Firewall-ներ՝** Enterprise Border, Data Center / Server-Farm, Zero Trust Network Access / User Access GW և WAN IPsec firewall-ներ:
- **Օպտիկական մոդուլներ և մալուխներ.** Բոլոր անհրաժեշտ SFP/SFP+/SFP28/QSFP+/QSFP28 օպտիկական մոդուլները և համատեղելի մալուխները սարքերի միջև լիարժեք կապի համար, ներառյալ մալուխային բաշխման համակարգերը (ODF-ներ, հորիզոնական և ուղղահայաց մալուխային կառավարիչներ):
- **Կենտրոնացված կառավարման և հաշվառման համակարգեր.** Կառավարման և հաշվառման սարքավորումներ:
- **Լրացուցիչ անվճար ծառայություններ** ՝ տեղադրման օգնություն, շահագործման հանձնում, ուսուցում և տեղադրումից հետո աջակցություն

Յուրաքանչյուր առաջարկ պետք է ներառի.

- Մանրամասն տեխնիկական բնութագրեր և տվյալների թերթիկներ:
- Սարքավորումների և ցանկացած լրացուցիչ ծառայությունների գները:
- Բոլոր լիցենզիաները՝ պահանջվող գործառույթները իրականացնելու համար:
- Երաշխիքի, աջակցության և ծրագրային ապահովման բաժանորդագրության պայմաններ:
- Համապատասխանության ապացույցներ (վկայագրեր, փորձարկման զեկույցներ):
- **Լրացուցիչ անվճար ծառայություններ.** Առաջին տեղը գրաված մասնակիցը (հաղթող մասնակից) պետք է ներկայացնի արտադրողի կողմից տրված Արտադրողի լիազորագրի ձևաթուղթ (MAF):

Տեխնիկական պահանջներ

Առաջարկվող բոլոր սարքավորումներն ու ծրագրային ապահովումը պետք էհամապատասխանեն հետևյալ ընդհանուր և սարքին բնորոշ պահանջներին: Մատակարարները պետք է տրամադրեն յուրաքանչյուր ապրանքի աջակցությունը հաստատող փաստաթղթեր

3.1 EVPN/VXLAN Fabric-ի ընդհանուր պահանջները

3.1.1 Երթուղային և կամուրջային կապ

EVPN Fabric տեղակայման համար սարքավորումները պետք է աջակցեն առաջադեմ 2-րդ և 3-րդ մակարդակի ֆունկցիոնալություններին, ներառյալ՝

1. Համապատասխանություն բոլոր անհրաժեշտ EVPN ստանդարտներին (օրինակ՝ RFC 7432, RFC 8365):
2. EVPN/VXLAN՝ երթուղայնացման և կամուրջների ստեղծման համար, հնարավորություն տալով համատեղել ցանցը:
3. Կենտրոնացված երթուղավորման և կամրջման (CRB) նախագծում տերևային անջատիչների վրա:
4. Բազմասարքային համակարգերի համակցում (MC-LAG)՝ բարձր մատչելիության համար:
5. Ethernet հատվածի նույնականացուցիչ (ESI) բազմամուտքային միացման համար:
6. Հավասար արժեքով բազմաուղի (ECMP)՝ մինչև 128 ուղիներով, գումարած անհավասար արժեքով բազմաուղի (UCMP) երթուղայնացում:
7. Սահմանային դարպասի արձանագրություն (BGP) դինամիկ երթուղավորման համար:
8. Երկկողմանի վերահասցեավորման հայտնաբերում (BFD)՝ խափանումների արագ հայտնաբերման համար:
9. Anycast IP հասցեավորում բեռի հավասարակշռման և հուսալիության համար:
10. Վիրտուալ MAC/IP հասցեավորում շարժունակության և ճկունության համար:
11. Քաղաքականության վրա հիմնված երթուղավորում (PBR) երթևեկության կառավարման համար:

3.1.2 Սարքավորումներ

Սարքավորումների բաղադրիչները պետք է ապահովեն բարձր արդյունավետություն և հուսալիություն.

1. 800 նվ կամ ավելի ցածր ASIC լատենտություն՝ գերցածր լատենտությամբ վերահասցեավորման համար:
2. Հավելյալ սնուցման աղբյուրներ՝ խափանումների նկատմամբ հանդուրժողականության ապահովման համար:
3. Ժամանակի համաժամեցման համար Precision Time Protocol (PTP)/IEEE 1588-ի աջակցություն:

3.1.3 Ծառայության որակ (QoS)

QoS գործառույթները պետք է կարգավորեն տրաֆիկի առաջնահերթությունը և գերբեռնվածության կառավարումը.

1. Միկրոանջատում հայտնաբերում՝ արտացոլելով կորցրած տրաֆիկը վերլուծության համար:
2. Աջակցություն ակնհայտ գերբեռնվածության մասին ծանուցման (ECN), տվյալների կենտրոնի կամուրջների փոխանակման (DCBX) և առաջնահերթ հոսքի կառավարման (PFC) համար:

3.1.4 Սպասարկում

Ծառայության սպասարկման հնարավորությունները պետք է նվազագույնի հասցնեն անսարքությունների ժամանակը և պարզեցնեն գործողությունները.

1. Բոլոր ցանցային մոդելների համար ընդհանուր ծրագրային պատկեր՝ հետևողական թարմացումների համար:
2. Միասնական կառավարման համար ընդհանուր մոնիթորինգի և մատակարարման գործիքներ:
3. Խելացի համակարգի արդիականացման (SSU) ֆունկցիոնալություն, ներառյալ ցանցի սպասարկման ռեժիմը կոմուտատորի վերագործարկման ժամանակ՝ տվյալների ցանցային ենթակառուցվածքի հասանելիությունը պահպանելու համար:

3.1.5 Հեռաչափման հավաքագրում

Հեռամետրիան պետք է կատարվի իրական ժամանակում՝ պատկերացում տալով ցանցի աշխատանքի վերաբերյալ.

4. Աջակցություն OpenTelemetry-ին՝ տվյալները InfluxDB կամ Prometheus արտահանելու հնարավորությամբ: Բոլոր հավաքագրող չափանիշների համար սկզբից հետո ինտերվալը 2 վայրկյան կամ պակաս է:
5. sFlow/IPFIX նմուշառում 1:500 հարաբերակցությամբ՝ հոսքի մոնիթորինգի համար:
6. Ներքին հեռաչափություն՝ փաթեթային մակարդակի վերաբերյալ մանրամասն պատկերացում կազմելու համար:

3.1.6 Անվտանգություն

Անվտանգության մեխանիզմները պետք է պաշտպանեն ցանցը սպառնալիքներից.

1. Վերահսկիչ հարթակի պաշտպանման քաղաքականություն (CoPP)՝ վերահսկիչ հարթակի ռեսուրսների պաշտպանությունը ապահովելու համար :
2. IPv4/IPv6 2-րդ շերտ/3-րդ շերտ/4-րդ շերտ մուտքի/ելքի կառավարման ցուցակներ (ACL):
3. : ACL-ով մերժված փաթեթների հաշվիչներ և մատյանագրում՝ աուդիտի նպատակով
4. Ինտեգրված փաթեթների գրավում՝ խնդիրների լուծման համար:
5. Անհատականացված իրադարձությունների հայտնաբերում և մշակում, որը աջակցում է CLI-ի և սկրիպտների վրա հիմնված ավտոմատացմանը:
6. Unicast հակադարձ ուղու վերահասցեավորում (uRPF)՝ կեղծումից պաշտպանվելու համար:
7. DHCP-ի աջակցությամբ MAC/IP անվտանգություն:

3.1.7 Մոնիթորինգ

Մոնիթորինգի լուծումը պետք է ապահովի կենտրոնացված կառավարման հարթակ, որը կապահովի ցանցային գործունեության պարզեցված փորձ: Այն պետք է օգտագործի ամպային ցանցային սկզբունքները ավտոմատացման, դիտարկելիության և անվտանգության համար: Հիմնական պահանջները ներառում են՝

- Տվյալների կենտրոններում, կամպուսներում և WAN տիրույթներում ցանցային սարքերի մոնիթորինգի, սպասարկման և կազմակերպման ամբողջական կառավարում:
- Հեռաչափման տվյալների անընդհատ հոսքը սարքերից՝ իրական ժամանակում պատկերացում կազմելու համար:

- Շրջակա միջավայրի մոնիթորինգ՝ ջերմաստիճանի, էլեկտրամատակարարման օգտագործման, օդափոխիչի արագության, ինտերֆեյսների կարգավիճակի և աշխատանքի գրաֆիկական ցուցադրումներով:
- Բարդ առաջադրանքների ավտոմատացում, ներառյալ կարգավորումների կառավարումը, համապատասխանության ստուգումները և առանց մարդկային միջամտության կարգավորում:
- Դիտարկելիության գործառույթներ, ինչպիսիք են գույքագրման հետևումը (օրինակ՝ հոսթի անունը, կառավարման IP հասցեն, սերիական համարները), տոպոլոգիայի վիզուալիզացիան և փոփոխությունների վերահսկումը:
- Շրոյական վստահության անվտանգության ինտեգրում, ներառյալ VXLAN ծածկույթների տեսանելիությունը և երրորդ կողմի սարքերի թարմացումները:
- Աջակցություն տեղական մոդելի համար:
- Անոմալիաների հայտնաբերման, կատարողականի միտումների գնահատման և կանխատեսողական սպասարկման համար առաջադեմ վերլուծություններ:

3.2 EVPN/VXLAN Fabric սարքին հատուկ պահանջներ

3.2.1 Միջուկային հիմնական (Spine) սարքեր

- 32 x 100GE QSFP28 միացքներ:
- Վիրտուալ ելքային հերթագրման (VoQ) ճարտարապետություն:
- 32 ՄԲ համօգտագործվող բուֆեր:
- Օդի հոսք՝ առջևից դեպի հետ

3.2.2 Եզրային (Leaf) սարքեր

Պահանջվում է երկու տարբերակ՝

- **Տարբերակ 1՝** 48 x 1/10GE Base-T միացքներ + 4 x 100GE վերբեռնման միացումներ
- **Տարբերակ 2՝** 48 x 10/25GE SFP28 միացք + 6 x 100GE վերբեռնման միացումներ
- Երկուսն էլ՝ Վիրտուալ ելքային հերթագրման (VoQ) ճարտարապետություն:
- Երկուսն էլ՝ 32 ՄԲ համատեղ օգտագործվող բուֆեր:
- Փոխանցման տեղեկատվական բազա (FIB). Մինչև 288 հազար MAC հասցե:
- FIB: Մինչև 360 հազար երթուղի:
- Օդի հոսք՝ առջևից դեպի հետ

3.2.3 Ծառայության թերթիկ/DCI սարքեր

- 48 x 10/25GE SFP28 միացք + 6 x 100GE միացք:
- Վիրտուալ ելքային հերթագրման (VoQ) ճարտարապետություն:
- 16 ԳԲ համօգտագործվող բուֆեր:
- FIB: Մինչև 256 հազար MAC հասցեներ:
- FIB: Մինչև 1.5 միլիոն երթուղիներ:

- ARP աղյուսակ՝ մինչև 80 հազար գրառում:
- DCI աջակցություն. EVPN/VXLAN-ից EVPN/MPLS փոխանցում փոխկապակցման համար
- Օդի հոսք՝ առջևից դեպի հետ

3.3.1 Քանակներ և աջակցություն

- Միջուկային հիմնական (Spine) սարքեր՝
    - 2 զույգ (ընդհանուր 4 սարք)՝ 5 տարվա աջակցությամբ և համապատասխան ծրագրային լիցենզիաներով:
    - Առաջադեմ սարքավորումների փոխարինում (RMA)՝ 24/7 TAC մուտքով:

- Եզրային (Leaf)անջատիչներ
    - Տարբերակ 1:
        - 4 զույգ + 1 պահեստային սարք (ընդհանուր 9 սարք)՝ 5 տարվա աջակցությամբ և համապատասխան ծրագրային ապահովման լիցենզիաներ:
        - Առաջադեմ սարքավորումների փոխարինում (RMA)՝ 24/7 TAC մուտքով:
    - Տարբերակ 2:
        - 5 զույգ + 1 պահեստային սարք (ընդհանուր 11 սարք)՝ 5 տարվա աջակցությամբ և համապատասխան ծրագրային ապահովման լիցենզիաներ:
        - Առաջադեմ սարքավորումների փոխարինում (RMA)՝ 24/7 TAC մուտքով:

- Ծառայության թերթիկ/DCI սարքեր (EVPN L3):
    - 2 զույգ (ընդհանուր 4 սարք)՝ 5 տարվա աջակցությամբ և համապատասխան ծրագրային լիցենզիաներով:
    - Առաջադեմ սարքավորումների փոխարինում (RMA)՝ 24/7 TAC մուտքով:

- Մոնիթորինգ և կառավարում.
    - HA տեղում տեղակայված վիրտուալ սարքերի զույգ՝ evpn/vlxan fabric սարքերի 5 տարվա բաժանորդագրության լիցենզիայով:

4. Ձեռնարկության սահմանային firewall-ներ, DC firewall-ներ և զրոյական վստահության ցանցային մուտք

4.1 Ձեռնարկության սահմանային firewall-ի նվազագույն պահանջները

- Ձևաչափ՝ դարակի վրա ամրացում, 1U 19" ստանդարտ դարակ
- Firewall-ի թողունակություն (եթե հավելվածի տեսանելիությունը և գրանցումը միացված են)՝ 8 Գբ/վ

- Սպառնալիքների կանխարգելման թողունակություն (եթե հավելվածի տեսանելիությունը, IPS-ը, AV-ը, AMP-ը և գրանցումը միացված են)՝ 4 Գբ/վ
- Միաժամանակյա սեսիաներ՝ 900 հազար
- Նոր սեսիաներ վայրկյանում: 100 հազար
- Վիրտուալ համակարգեր/դոմեններ (ամբողջական վիրտուալ կտրում անկախ կառավարմամբ). առնվազն 5
- Վիրտուալ երթուղայնացման և վերահասցեավորման աղյուսակներ՝ առնվազն 10
- Ուղղորդում. BGP՝ նրբագեղ վերագործարկմամբ, քաղաքականության վրա հիմնված վերահասցեավորում, BFD
- Ինտերֆեյսի ռեժիմներ՝ L2, L3, թակ, վիրտուալ լար
- Ինտերֆեյսի տեսակներ՝ 8 x 1/10G RJ45, 4 x 1/10G SFP/SFP+, 1 x 1/10G SFP/SFP+ HA
- Կլաստերացում՝ Ակտիվ/Ակտիվ, Ակտիվ/Պասիվ, հորիզոնական մասշտաբավորում (մինչև 4 սարք)
- Ներկառուցված պահեստավորում՝ ավելի քան 250 ԳԲ SSD
- Երկակի AC սնուցման աղբյուր՝ 1+1 ավելորդության համար. հնարավոր է փոխարինել տաք ռեժիմով
- Օդի հոսք՝ առջևից-հետև

4.2 Տվյալների կենտրոնի / սերվերների ֆերմայի firewall-ի նվազագույն պահանջները

- Ձևաչափ՝ դարակի վրա ամրացում, 1U 19" ստանդարտ դարակ
- Firewall-ի թողունակություն (եթե հավելվածի տեսանելիությունը և գրանցումը միացված են)՝ 19 Գբ/վ
- Սպառնալիքների կանխարգելման թողունակություն (եթե հավելվածի տեսանելիությունը, IPS-ը, AV-ը, AMP-ը և գրանցումը միացված են)՝ 10 Գբ/վ
- Միաժամանակյա սեսիաներ՝ 2 միլիոն
- Նոր սեսիաներ վայրկյանում: 200 հազար
- Վիրտուալ համակարգեր/դոմեններ (ամբողջական վիրտուալ բաժանում անկախ կառավարմամբ). առնվազն 10
- Վիրտուալ երթուղայնացման և վերահասցեավորման աղյուսակներ՝ առնվազն 10
- Ուղղորդում. BGP՝ նրբագեղ վերագործարկմամբ, քաղաքականության վրա հիմնված վերահասցեավորում, BFD
- Ինտերֆեյսի ռեժիմներ՝ L2, L3, թակ, վիրտուալ լար
- Կլաստերացում՝ Ակտիվ/Ակտիվ, Ակտիվ/Պասիվ, հորիզոնական մասշտաբավորում (մինչև 4 սարք)
- VXLAN թունելի ստուգում
- Ինտերֆեյսի տեսակներ՝ 8 x 1/10G RJ45, 4 x 1/10G SFP/SFP+, 4 x 25G SFP28+, 1 x 1/10G SFP/SFP+ HA
- Ներկառուցված պահեստավորում՝ ավելի քան 250 ԳԲ SSD
- Երկակի AC սնուցման աղբյուր՝ 1+1 ավելորդության համար. հնարավոր է փոխարինել տաք ռեժիմով
- Օդի հոսք՝ առջևից-հետև

4.3 Campus Zero Trust Network Access Firewall / User Access GW պահանջները

- Ձևաչափ՝ դարակի վրա ամրացում, 1U 19" ստանդարտ դարակ
- Firewall-ի թողունակություն (եթե հավելվածի տեսանելիությունը և գրանցումը միացված են)՝ 19 Գբ/վ
- Սպառնալիքների կանխարգելման թողունակություն (եթե հավելվածի տեսանելիությունը, IPS-ը, AV-ը, AMP-ը և գրանցումը միացված են)՝ 10 Գբ/վ
- Միաժամանակյա նիստեր՝ 2 միլիոն
- Նոր սեսիաներ վայրկյանում: 200 հազար
- Հաճախորդի SSL VPN թունելների նվազագույն քանակը՝ 1500
- Վիրտուալ համակարգեր/դոմեններ (ամբողջական վիրտուալ կտրում անկախ կառավարմամբ). առնվազն 5
- Վիրտուալ երթուղայնացման և վերահասցեավորման աղյուսակներ՝ առնվազն 10
- Ուղղորդում. BGP՝ նրբագեղ վերագործարկմամբ, քաղաքականության վրա հիմնված վերահասցեավորում, BFD
- Ինտերֆեյսի ռեժիմներ՝ L2, L3, թակ, վիրտուալ լար
- Ինտերֆեյսի տեսակներ՝ 8 x 1/10G RJ45, 4 x 1/10G SFP/SFP+, 4 x 25G SFP28+, 1 x 1/10G SFP/SFP+ HA
- Կլաստերացում՝ Ակտիվ/Ակտիվ, Ակտիվ/Պասիվ, հորիզոնական մասշտաբավորում (մինչև 4 սարք)
- Ներկառուցված պահեստավորում՝ ավելի քան 250 ԳԲ SSD
- Երկակի AC սնուցման աղբյուր՝ 1+1 ավելորդության համար. հնարավոր է փոխարինել տաք ռեժիմով
- Օդի հոսք՝ առջևից-հետ

Firewall-ների ընդհանուր պահանջները.

- Firewall-ի միջուկում ներկառուցված մեքենայական ուսուցման մեխանիզմ՝ստորագրության չպահանջող սպառնալիքների հայտնաբերման համար
- Իրական ժամանակի SSL ստուգում (ներառյալ TLS 1.3)՝ հարձակման ողջ մակերեսին օգտատերերի, սարքերի և ծրագրերի վերաբերյալ լիարժեք տեսանելիություն ապահովելու համար:
- Պետական firewall, ներխուժումների կանխարգելման համակարգ (IPS), վնասակար ծրագրերից պաշտպանություն և ծրագրերի վերահսկում, անվտանգության քաղաքականության կիրառում:
- Ինտեգրացիա նույնականացման ծառայությունների հետ, ինչպիսին է Active Directory-ն,՝ օգտատիրոջ ինքնության և խմբային անդամակցության վրա հիմնված անվտանգության քաղաքականությունները կիրառելու համար:
- VXLAN թունելի ստուգման հնարավորություն:
- Firewall-ի մատակարարը պետք է ունենա VM-ի վրա հիմնված և կոնտեյներային վիրտուալ սարքավորումներ՝ վիրտուալացված միջավայրը (ESXi, KVM, HyperV, AHV) և կոնտեյներային միջավայրը (Kubernetes) պաշտպանելու համար: Ըստ ցանկության:

Լրացուցիչ պահանջներ Campus Zero Trust Firewall-ների համար

Firewall-ի ընդհանուր պահանջները, գումարած՝

- Անձնագրային մուտքի վերահսկում
- Նվազագույն մուտքի արտոնությունների մոդել
- Վստահության շարունակական գնահատում նիստերի ընթացքում
- Կենտրոնացված քաղաքականության վրա հիմնված մուտքի վերահսկողություն
- Կիրառական մակարդակի միկրոսեգմենտացիա
- Ինտեգրացիա բազմագործոն նույնականացման (MFA) հետ
- Աջակցություն SAML, OIDC և OAuth2-ի վրա հիմնված SSO-ի համար
- Ինտեգրացիա LDAP-ի, AD-ի, Azure AD-ի և ինքնության մատակարարների հետ
- Բազմապլատֆորմային աջակցություն (Windows, macOS, Linux, iOS և Android)
- Սարքի դիրքի գնահատում և համապատասխանության ստուգում

4.4 Քանակներ և աջակցություն

- Ձեռնարկության սահմանային firewall-ներ.
    - 2 զույգ NGFW (ընդհանուր 4 սարք) HA կոնֆիգուրացիայում:
    - 3 կամ 5 տարվա աջակցություն՝ լիարժեք անվտանգության բաժանորդագրություններով (TP, URL, DNS, ամպային sandboxing):
- Տվյալների կենտրոնի / սերվերների ֆերմայի firewall-ներ՝
    - 2 զույգ NGFW (ընդհանուր 4 սարք) HA կոնֆիգուրացիայում:
    - 3 կամ 5 տարվա աջակցություն՝ VXLAN ստուգման հնարավորությամբ:
- Campus Zero Trust Network Access Firewall-ներ՝
    - 2 զույգ (ընդհանուր 4 սարք) HA կոնֆիգուրացիայում:
    - 3 կամ 5 տարվա աջակցություն SSL VPN-ով և հոսթի տեղեկատվության հավաքագրմամբ:

---

5. Կենտրոնացված կառավարում և գրանցում

5.1 Պահանջներ

- Ձևի գործոն՝ վիրտուալ սարք:
- Աջակցվող հիպերվիզորներ՝ VMware ESXi, KVM, Nutanix, Microsoft Hyper-V:
- Կլաստերացում՝ ակտիվ/պասիվ:
- Գրանցամատյանի պահպանում՝ ≥ 3 ամիս:
- Գրանցամատյանների հավաքագրում՝ ≥ 25,000 գրանցամատյան/վայրկյան մեկ օրինակի համար:
- Բաշխված գրանցամատյանների հավաքագրիչի տեղակայման աջակցություն:
- Շաբլոններում սահմանված կոնֆիգուրացիայի բաղադրիչների փոփոխականներ

- Սարքերի բազմամակարդակ խմբավորում կենտրոնացված կերպով քաղաքականությունների և օբյեկտների բոլոր տեղակայումներումները կառավարելու համար:
- Դերերի վրա հիմնված մուտքի վերահսկողություն, հաշվետվություններ և ծրագրաշարի/լիցենզիայի թարմացումների կառավարումը վերահսկվող սարքերի համար:
- Սարքավորումների, վիրտուալ սարքավորումների և կոնտեյներային սարքավորումների համար ընդհանուր կառավարում, մոնիթորինգ և գրանցամատյանների հավաքագրում:

5.2 Քանակներ և աջակցություն

- **Կենտրոնացված կառավարում և գրանցում.**
    - 1 HA զույգ սարքերի կառավարման համար (մինչև 25 սարք):
    - 1 HA զույգ՝ նվիրված գերանների հավաքման համար:
    - 5 տարվա աջակցություն սարքերի կառավարչի և գրանցամատյանների հավաքագրողի համար:

---

6. Ձեռնարկության WAN IPsec Firewall-ներ

6.1 Firewall-ի պահանջները

- Ռելսային ամրացման համար մինչև 2U, 19 դյույմ ստանդարտ
- IPsec VPN թողունակություն՝ ≥ 45 Գբ/վ (AES256-SHA256)
- Կայքից կայք VPN թունելներ՝ ≥ 15,000
- Միաժամանակյա սեանսներ՝ ≥ 9 միլիոն
- Նոր սեսիաներ վայրկյանում. ≥ 500 հազար
- Վիրտուալ համակարգեր՝ մինչև 250
- Երթուղարկում՝ BGP, PBF, BFD
- Ինտերֆեյսի ռեժիմներ՝ L2, L3
- Ինտերֆեյսներ՝ 16 x GE RJ45, 8 x GE SFP, 12 x 10/25G SFP+/SFP28, 4 x 40/100G QSFP+/QSFP28
- Երկու տաք փոխարինման հնարավորությամբ սնուցման բլոկներ
- առջևից դեպի ետ օդային հոսք

6.2 Կենտրոնացված կառավարում և գրանցում

- Ձևի գործոն՝ վիրտուալ սարք:
- Աջակցվող հիպերվիզորներ՝ VMware ESXi, KVM, Nutanix, Microsoft Hyper-V:
- Ակտիվ/պասիվ կլաստերացում:
- Բաշխված գրանցամատյանների հավաքագրում և քաղաքականության վրա հիմնված լիարժեք կառավարում:

6.3 Քանակներ և աջակցություն

- Ձեռնարկության WAN Firewall-ներ՝
    - 2 զույգ (ընդհանուր 4 սարք)՝ 5 տարվա աջակցությամբ:
- Կենտրոնացված կառավարում և գրանցում.
    - 1 HA զույգ, որը կառավարում է մինչև 100 սարք՝ 5 տարվա աջակցությամբ:

---

7. Օպտիկական փոխանցող-հաղորդիչներ

7.1 Օպտիկական մոդուլներ

Մասնակիցները պետք է ապահովեն բոլոր անհրաժեշտ օպտիկական ընդունիչները՝ ծայրից ծայր կապն ապահովելու համար:

- SFP+ (10G), SFP28 (25G), QSFP+/QSFP28 (40G/100G):
- Մոդուլները պետք է համապատասխանեն կոմուտատորի և firewall-ի ինտերֆեյսի պահանջներին և համատեղելի լինեն համապատասխան սարքերի հետ:
- Աջակցություն կարճաժամկետ (SR) և երկարաժամկետ (LR) օպտիկայի համար՝ կախված տեղակայման դիզայնից:

7.2 Քանակներ

- 10GBASE-T SFP+ պղինձ (նվազագույնը 30 մ):
    - Ընդհանուր 20 միավոր - 16 միավոր համատեղելի է 4.4 սարք, 4 միավոր համատեղելի 3.3.1 սարքերի հետ
- 10GBASE-LR SFP+ Դուպլեքս LC/UPC SMF:
    - 200 միավոր՝ 160 միավոր համատեղելի 3.3.1 սարքերի հետ, 20 միավոր համատեղելի 4.4 սարքերի հետ, 20 միավոր համատեղելի 6.3 սարքերի հետ
- 25GBASE-LR SFP28 դուպլեքս LC/UPC SMF:
    - Ընդհանուր առմամբ 160 միավոր՝ 30 միավոր համատեղելի 4.4 սարքերի հետ, 40 միավոր համատեղելի 6.3 սարքերի հետ, 90 միավոր համատեղելի 3.3.1 սարքեր
- 100GBASE-DR QSFP28 Դուպլեքս LC/UPC SMF:
    - 64 միավոր ՝ 56 միավոր համատեղելի 3.3.1 սարքերի հետ , 8 միավոր համատեղելի 6.3 սարքեր
- 100GBASE-PSM4 QSFP28 MPO-12 SMF:
    - 24 միավոր՝ լիովին համատեղելի 3.3.1 սարքերի հետ