**ნაწილი 1: როუტერის უსაფრთხოება**

**1. რატომ არის საჭირო edge router-ის დაცვა?**

ა) Edge router მოძველებული ტექნოლოგიაა და საჭიროებს დამატებით დაცვას

**ბ) Edge router წარმოადგენს ქსელის პირველ შეხების წერტილს ინტერნეტთან ან სხვა არაუსაფრთხო ქსელთან**

გ) Edge router-ის დაცვა მხოლოდ დიდი კორპორაციებისთვისაა მნიშვნელოვანი

დ) Edge router-ის დაცვა არ არის პრიორიტეტული ამოცანა

**2. რა უპირატესობა აქვს "Defense in Depth" მიდგომას "Single Router" მიდგომასთან შედარებით?**

**ა) Defense in Depth იყენებს მრავალფენიან დაცვას, რაც ართულებს თავდამსხმელისთვის სისტემის გარღვევას**

ბ) Defense in Depth არის უფრო იაფი გადაწყვეტილება

გ) Defense in Depth საჭიროებს ნაკლებ ტექნიკურ ცოდნას

დ) Defense in Depth ამცირებს ქსელის სიჩქარეს, მაგრამ ზრდის უსაფრთხოებას

**3. რომელია სამი ძირითადი ასპექტი როუტერის უსაფრთხოებაზე?**

ა) ფიზიკური დაცვა, პროგრამული უზრუნველყოფა, ქსელის მონიტორინგი

**ბ) ფიზიკური დაცვა, ადმინისტრაციული წვდომის კონტროლი, კონფიგურაციის და ოპერაციული დაცვის უზრუნველყოფა**

გ) კონფიდენციალურობა, მთლიანობა, ხელმისაწვდომობა

დ) ფაირვოლი, ანტივირუსი, შიფრაცია

**4. რატომ არის აუცილებელი მენეჯმენტ არხზე დაშიფრული პროტოკოლების გამოყენება?**

ა) დაუშიფრავი პროტოკოლები აჩქარებენ მართვის პროცესს

ბ) დაშიფრული პროტოკოლები ამცირებენ ქსელის დატვირთვას

**გ) დაუშიფრავი პროტოკოლებით მენეჯმენტზე წვდომა ხდის მოწყობილობას მოწყვლადს Man-in-the-Middle შეტევების მიმართ**

დ) დაშიფრული პროტოკოლები უზრუნველყოფენ უკეთეს მხარდაჭერას პრობლემების გადაჭრისას

**5. რატომ უნდა გამოვიყენოთ ძლიერი პაროლები მოწყობილობებზე?**

ა) ძლიერი პაროლები საშუალებას გვაძლევს უფრო იშვიათად შევცვალოთ ისინი

**ბ) ძლიერი პაროლები ართულებს დაუმტკიცებელი წვდომის მცდელობებს და იცავს მოწყობილობას brute-force და dictionary ტიპის შეტევებისგან**

გ) ძლიერი პაროლები უზრუნველყოფენ უფრო სწრაფ აუთენტიფიკაციას

დ) ძლიერი პაროლები მხოლოდ რეკომენდებულია, მაგრამ არ არის აუცილებელი

**6. რით განსხვავდება "enable password" და "enable secret" Cisco მოწყობილობებში?**

ა) enable password უფრო ადვილი დასამახსოვრებელია, ხოლო enable secret რთული

ბ) enable password გამოიყენება მხოლოდ კონსოლიდან შესვლისას, ხოლო enable secret რემოტულად შესვლისას

**გ) enable password ინახება უმარტივესი ტექსტური ფორმით, ხოლო enable secret ინახება დაშიფრულად**

დ) enable password არ საჭიროებს განახლებას, ხოლო enable secret პერიოდულად უნდა შეიცვალოს

**7. როგორ მუშაობს login blocking მექანიზმი Cisco მოწყობილობებზე?**

ა) ავტომატურად ცვლის პაროლებს განსაზღვრული დროის შემდეგ

**ბ) აყოვნებს ან ბლოკავს შემდგომი ავტორიზაციის მცდელობებს გარკვეული რაოდენობის წარუმატებელი ლოგინების შემდეგ**

გ) ბლოკავს მხოლოდ გარე IP მისამართებიდან წვდომას

დ) ავტომატურად ჩართავს დამატებით აუთენტიფიკაციის ფაქტორს შესვლის მცდელობებისას

**8. რისთვის გამოიყენება SSH კონფიგურაცია Cisco მოწყობილობებში?**

ა**) უზრუნველყოფს დისტანციური მართვის სესიებს დაშიფრული არხის გამოყენებით**

ბ) ზრდის მოწყობილობის შესრულების მაჩვენებლებს

გ) ამარტივებს მოწყობილობის კონფიგურაციას

დ) ავტომატურად ანაწილებს ქსელის რესურსებს

**9. რატომ არის საჭირო privilege level-ების კონფიგურაცია?**

ა) უზრუნველყოფს სწრაფ წვდომას ყველა ფუნქციაზე

ბ) ამარტივებს მოწყობილობის კონფიგურაციას

**გ) საშუალებას აძლევს ადმინისტრატორს გაანაწილოს მომხმარებლების უფლებები და მათზე მხოლოდ აუცილებელი ბრძანებები გააკეთოს ხელმისაწვდომი**

დ) საშუალებას იძლევა დავაფიქსიროთ, თუ ვინ რა ცვლილებები შეიტანა სისტემაში

**10. რა არის Role-Based CLI და რატომ ვიყენებთ მას?**

ა) უზრუნველყოფს ავტომატურ კონფიგურაციას სხვადასხვა როლისთვის

**ბ) საშუალებას იძლევა გავყოთ ბრძანებების ჯგუფები სხვადასხვა როლისთვის, რაც აუმჯობესებს მენეჯმენტს და ზრდის უსაფრთხოებას**

გ) ამარტივებს CLI ინტერფეისს დამწყები მომხმარებლებისთვის

დ) ავტომატურად ცვლის მომხმარებლის პრივილეგიებს სხვადასხვა დროის მონაკვეთში

**ნაწილი 2: როუტერის უსაფრთხოების დამატებითი ასპექტები**

**11. რატომ არის მნიშვნელოვანი IOS resilient configuration-ის ჩართვა?**

ა) IOS resilient configuration ზრდის მოწყობილობის წარმადობას

**ბ) Resilient configuration ინახავს კრიტიკულ ფაილებს სპეციალურ, დაცულ ადგილას მეხსიერებაში**

გ) Resilient configuration ამარტივებს მოწყობილობის ყოველდღიურ მართვას

დ) IOS resilient configuration საშუალებას იძლევა დავზოგოთ მეხსიერება მოწყობილობაზე

**12. რა განსხვავებაა In-band და Out-of-band მენეჯმენტს შორის?**

ა) In-band მენეჯმენტი უფრო დაცულია, ვიდრე Out-of-band

ბ) In-band მენეჯმენტი უფრო ძვირია, ვიდრე Out-of-band

**გ) In-band — მოწყობილობის მართვა ხდება იგივე ქსელით, რაც მომხმარებლების მონაცემებისთვის გამოიყენება, ხოლო Out-of-band — მართვისთვის გამოიყენება ცალკე კომუნიკაციის არხი**

დ) In-band მენეჯმენტი საჭიროებს სპეციალურ აპარატურას, მაშინ როცა Out-of-band იყენებს სტანდარტულ მოწყობილობებს

**13. როგორ მუშაობს Syslog და რატომ არის ის მნიშვნელოვანი?**

ა) Syslog ახდენს მოწყობილობის ავტომატურ განახლებას და უსაფრთხოების პროგრამების ინსტალაციას

**ბ) Syslog აგროვებს და აგზავნის ქსელური მოწყობილობების მიერ გენერირებულ შეტყობინებებს ცენტრალურ სერვერზე**

გ) Syslog ახდენს მოწყობილობის კონფიგურაციის ავტომატურ შენახვას

დ) Syslog უზრუნველყოფს მომხმარებლების ავტომატურ აუთენტიფიკაციას სხვადასხვა მოწყობილობებზე

**14. რატომ არის SNMPv3 აუცილებელი SNMPv1 ან SNMPv2-ის ნაცვლად?**

ა) SNMPv3 უფრო სწრაფია და ეფექტურია

**ბ) SNMPv3 მხარს უჭერს ავთენტიფიკაციას და დაშიფვრას**

გ) SNMPv3 უფრო ადვილი დასაკონფიგურირებელია

დ) SNMPv3 არ საჭიროებს სპეციალურ აპარატურას განსხვავებით წინა ვერსიებისგან

**15. რატომ უნდა დაიყოს NTP-ის დროის წყაროები სექრეტული წყაროებიდან?**

ა) სექრეტული წყაროები უფრო ზუსტ დროს იძლევიან

ბ) დროის წყაროების დაყოფა ზრდის მოწყობილობის წარმადობას

**გ) სექრეტული წყაროებიდან მიღებული დრო ამცირებს spoofed (გაყალბებული) დროის შეტევების რისკს**

დ) NTP-ის დროის წყაროები სუსტად არიან დაცულები და ყოველთვის საჭიროებენ დამატებით დაცვას

**16. როგორ მუშაობს AutoSecure ფუნქცია?**

ა) ავტომატურად ბლოკავს საეჭვო IP მისამართებს

**ბ) აწესრიგებს მოწყობილობაზე უსაფრთხოების კონფიგურაციას, დეაქტივირებს არასაჭირო სერვისებს**

გ) ავტომატურად განაახლებს მოწყობილობის პროგრამულ უზრუნველყოფას

დ) ახდენს ქსელის აუდიტს და აგზავნის შეტყობინებებს უსაფრთხოების პრობლემებზე

**17. რატომ არის Routing Protocol Authentication აუცილებელი OSPF-ში?**

ა) Authentication ზრდის OSPF-ის სიჩქარესა და ეფექტურობას

**ბ) Authentication იცავს როუტინგის ინფორმაციას არავარგისი მოწყობილობებისგან**

გ) Authentication ამარტივებს OSPF კონფიგურაციას

დ) OSPF Authentication არ არის აუცილებელი მცირე ქსელებში

**18. რა არის Control Plane Policing (CoPP) და როგორ იცავს ის მოწყობილობას?**

ა) CoPP ახდენს ქსელური პაკეტების შინაარსის ანალიზს მავნე კოდის აღმოსაჩენად

**ბ) CoPP ფილტრავს და ლიმიტირებს იმ ტრაფიკს, რომელიც მიდის მოწყობილობის control plane-ზე**

გ) CoPP ავტომატურად ბლოკავს არაავტორიზებულ მომხმარებლებს

დ) CoPP აკონტროლებს მართვის პანელის წვდომას ფიზიკურ დონეზე

**ნაწილი 3: Layer 2 (Switch) უსაფრთხოება**

**19. რა საფრთხეებია დამახასიათებელი Layer 2 (Switch) ქსელისთვის?**

ა) მხოლოდ DoS შეტევები

**ბ) CAM Table Overflow, VLAN Hopping, DHCP spoofing და starvation, ARP spoofing/poisoning, IP source spoofing, STP manipulation**

გ) მხოლოდ პაროლების მოპარვა და უნებართვო წვდომა

დ) Layer 2 ქსელი პრაქტიკულად დაუცველია სხვადასხვა ტიპის თავდასხმებისგან

**20. რა არის CAM Table Overflow შეტევა და როგორ მოქმედებს ის?**

**ა) თავდამსხმელი ავსებს switch-ის CAM table-ს ყალბი MAC მისამართებით, რის შედეგად switch იწყებს ყველა პაკეტის broadcast რეჟიმში გაგზავნას**

ბ) Switch მეხსიერება ივსება და იწვევს მის გადატვირთვას

გ) CAM Table Overflow ხდება მხოლოდ ძველ switch-ებზე

დ) Switch იწყებს შემთხვევითი პაკეტების გაგზავნას ყველა მიმართულებით

**21. როგორ შეიძლება CAM Table შეტევისგან დაცვა?**

ა) მხოლოდ ძვირადღირებული მოწყობილობების გამოყენებით

**ბ) Port Security-ის ჩართვით: მაქსიმალური MAC-ების რაოდენობის შეზღუდვა, სტატიკური MAC მისამართების რეგისტრაცია**

გ) მხოლოდ ფირმვეარის რეგულარული განახლებით

დ) CAM Table შეტევა ვერ არის თავიდან აცილებული თანამედროვე ქსელებში

**22. რას ნიშნავს Port Security-ის Protect, Restrict და Shutdown რეჟიმები?**

ა) Protect — იცავს MAC მისამართებს, Restrict — ზღუდავს კავშირის სიჩქარეს, Shutdown — გამორთავს პორტს გარკვეული დროით

**ბ) Protect — ჩუმად წყვეტს დაუმტკიცებელ MAC-ის პაკეტებს, Restrict — წყვეტს და აგზავნის log შეტყობინებას, Shutdown — პორტს აყენებს "error-disabled" მდგომარეობაში**

გ) Protect — სუსტი დაცვა, Restrict — საშუალო დაცვა, Shutdown — ძლიერი დაცვა

დ) ეს რეჟიმები განსხვავდებიან მხოლოდ შეტყობინებების გენერირების ხარისხით

**23. როგორია Port Security Aging მექანიზმის მუშაობა?**

ა) აძველებს მოწყობილობის პროგრამულ უზრუნველყოფას გარკვეული დროის შემდეგ

**ბ) Port Security Aging ავტომატურად შლის MAC მისამართებს მითითებული დროის გასვლის შემდეგ**

გ) ავტომატურად განაახლებს დაცვის მექანიზმებს

დ) ამოწმებს პორტის აქტიურობას და გამორთავს მას უმოქმედობის შემთხვევაში

**24. რატომ არის VLAN hopping შეტევა საშიში?**

ა) იწვევს მოწყობილობის გადატვირთვას

**ბ) VLAN hopping საშუალებას აძლევს თავდამსხმელს გადაკვეთოს VLAN ბარიერები და არაუფლებრივ VLAN-ებში მოხვდეს**

გ) ანელებს ქსელის მუშაობას

დ) ცვლის VLAN კონფიგურაციას

**25. როგორ უნდა დავიცვათ ქსელი VLAN hopping-ისგან?**

ა) უნდა გამოვიყენოთ მხოლოდ ერთი VLAN

**ბ) ყველა არაპირველადი პორტი დავაყენოთ access mode-ზე, დავუკეტოთ DTP, გამოვიყენოთ ვალიდური Native VLAN-id-ები**

გ) უნდა გამოვიყენოთ მხოლოდ უახლესი მოწყობილობები

დ) საჭიროა დამატებითი ფაირვოლის ინსტალაცია

**26. რა არის DHCP Spoofing შეტევა?**

ა) თავდამსხმელი ცვლის DHCP სერვერის IP მისამართს

ბ) DHCP სერვერი იწყებს გამოსაყენებელი IP მისამართების სწრაფ ამოწურვას

**გ) თავდამსხმელი აწარმოებს ყალბ DHCP სერვერს და აძლევს შეცდომით მისამართებს (default gateway, DNS)**

დ) თავდამსხმელი იპარავს DHCP სერვერის კონფიგურაციას

**27. როგორ ვებრძოლოთ DHCP Spoofing შეტევას?**

ა) უნდა გამოვიყენოთ სტატიკური IP მისამართები

**ბ) DHCP Snooping-ის ჩართვით: სანდო და არასანდო პორტების განსაზღვრით**

გ) ფაირვოლის გამოყენებით

დ) DHCP სერვერის რეგულარული გადატვირთვით

**28. რა ხდება DHCP Starvation შეტევისას?**

ა) DHCP სერვერი იცლება ფიზიკურად

**ბ) თავდამსხმელი ავსებს DHCP სერვერის მისამართების პულს ყალბი მოთხოვნებით (DISCOVER)**

გ) DHCP სერვერი ანელებს IP მისამართების გაცემას

დ) მომხმარებლები კარგავენ DHCP სერვერთან წვდომას ფიზიკურად

**29. როგორ მუშაობს ARP Spoofing შეტევა?**

**ა) თავდამსხმელი აგზავნის ყალბ ARP პასუხებს, აყალბებს MAC-IP ასოციაციას ქსელში**

ბ) ARP პროტოკოლი იწყებს შეფერხებით მუშაობას

გ) თავდამსხმელი ცვლის ARP ცხრილს მხოლოდ switch-ზე

დ) თავდამსხმელი ბლოკავს ARP მოთხოვნებს ქსელში

**30. როგორ ვიცავთ ქსელს ARP spoofing-ისგან?**

ა) მხოლოდ სტატიკური ARP ჩანაწერების გამოყენებით

**ბ) Dynamic ARP Inspection (DAI) გამოყენებით: შედარება DHCP snooping binding table-თან**

გ) ARP პროტოკოლის გამორთვით

დ) მხოლოდ IPv6 პროტოკოლის გამოყენებით

**31. რა არის IP Source Guard და როგორ მუშაობს?**

ა) IP Source Guard ფილტრავს პაკეტებს წყარო IP მისამართის მიხედვით

ბ) IP Source Guard არის პროგრამული უზრუნველყოფა, რომელიც იცავს IP მისამართებს

**გ) IP Source Guard ფილტრავს პაკეტებს და შეზღუდავს IP და MAC მისამართის spoofing შეტევებს**

დ) IP Source Guard წარმოადგენს ფიზიკურ მოწყობილობას

**32. რა საფრთხეებია დაკავშირებული Spanning Tree Protocol-თან (STP)?**

ა) STP არ არის დაკავშირებული უსაფრთხოების საფრთხეებთან

ბ) თავდამსხმელს შეუძლია მხოლოდ STP-ს გამორთვა

**გ) თავდამსხმელმა შეიძლება გააგზავნოს ყალბი BPDU შეტყობინებები და დაინიშნოს Root Bridge-ად**

დ) STP საფრთხეები მოქმედებენ მხოლოდ უსადენო ქსელებზე

**33. როგორ უნდა დავიცვათ STP ინფრასტრუქტურა?**

ა) STP-ს გამორთვით

**ბ) BPDU Guard, Root Guard, Loop Guard, PortFast გამოყენებით**

გ) მხოლოდ ერთი Root Bridge-ის გამოყენებით

დ) STP ინფრასტრუქტურის დაცვა შეუძლებელია

**34. რა ფუნქცია აქვს Private VLAN (PVLAN)-ს?**

ა) PVLAN არის უსაფრთხო VLAN განსაკუთრებით მნიშვნელოვანი მონაცემებისთვის

**ბ) PVLAN ხელს უშლის იმავე VLAN-ში მყოფ მოწყობილობებს ერთმანეთთან პირდაპირ კომუნიკაციაში ყოფნას**

გ) PVLAN ზრდის VLAN-ის წარმადობას

დ) PVLAN უზრუნველყოფს VLAN-ებს შორის იზოლაციას

**35. როგორია DHCP Snooping-ის კონფიგურაციის ძირითადი ნაბიჯები?**

ა) DHCP სერვერის დაყენება, კლიენტების კონფიგურაცია, ფაირვოლის დაყენება

**ბ) DHCP Snooping-ის აქტივაცია ვლანზე, სანდო პორტების მონიშვნა, სიჩქარის ლიმიტების დაყენება untrusted პორტებზე**

გ) DHCP სერვერის გამორთვა და ჩართვა, ახალი კონფიგურაციის ჩატვირთვა

დ) ქსელის მონიტორინგი, DHCP ტრაფიკის ანალიზი, პრობლემების აღმოჩენა

**36. რას გულისხმობს VLAN Double-Tagging შეტევა?**

ა) თავდამსხმელი იყენებს ორ VLAN-ს ტრაფიკის გადასაადგილებლად

**ბ) თავდამსხმელი ორ წარწერას (Tag) უმატებს Ethernet ჩარჩოს — Switch პირველი ტეგს აშორებს, მეორე კი რჩება**

გ) VLAN-ის კონფიგურაცია ორჯერ მეორდება

დ) შეტევა მიმართულია მხოლოდ ორი VLAN-ის წინააღმდეგ

//////////////////////////////////////////////////////////////////////////////////////////////////////////////////

1. რატომ არის საჭირო edge router-ის დაცვა?

პასუხი:

Edge router წარმოადგენს ქსელის პირველ შეხების წერტილს ინტერნეტთან ან სხვა არაუსაფრთხო ქსელთან. თუ იგი დაუცველია, თავდამსხმელმა ადვილად შეძლებს შიდა ქსელში შეღწევას ან შეტევების განხორციელებას.

2. რა უპირატესობა აქვს "Defense in Depth" მიდგომას "Single Router" მიდგომასთან შედარებით?

პასუხი:

Defense in Depth იყენებს მრავალფენიან დაცვას, რაც ართულებს თავდამსხმელისთვის სისტემის გარღვევას, მაშინ როცა Single Router მიდგომა მხოლოდ ერთ მოწყობილობაზეა დამოკიდებული.

3. როგორია სამი ძირითადი ასპექტი როუტერის უსაფრთხოებაზე?

პასუხი:

ფიზიკური დაცვა (Physical security)

ადმინისტრაციული წვდომის კონტროლი (Administrative access control)

კონფიგურაციის და ოპერაციული დაცვის უზრუნველყოფა (Operational security)

4. რატომ არის აუცილებელი მენეჯმენტ არხზე დაშიფრული პროტოკოლების გამოყენება?

პასუხი:

დაუშიფრავი პროტოკოლებით (მაგ., Telnet) მენეჯმენტზე წვდომა ხდის მოწყობილობას მოწყვლადს Man-in-the-Middle შეტევების მიმართ, ხოლო დაშიფრული პროტოკოლები (მაგ., SSH, HTTPS) უზრუნველყოფს მონაცემების

კონფიდენციალობასა და მთლიანობას.

5. რატომ უნდა გამოვიყენოთ ძლიერი პაროლები მოწყობილობებზე?

პასუხი:

ძლიერი პაროლები ართულებს დაუმტკიცებელი წვდომის მცდელობებს და იცავს მოწყობილობას brute-force და dictionary ტიპის შეტევებისგან.

6. რით განსხვავდება "enable password" და "enable secret" Cisco მოწყობილობებში?

პასუხი:

enable password ინახება მოწყობილობაზე უმარტივესი ტექსტური ფორმით (unencrypted).

enable secret ინახება მოწყობილობაზე დაშიფრულად, რაც უფრო მაღალი უსაფრთხოების დონეს იძლევა.

7. როგორ მუშაობს login blocking მექანიზმი Cisco მოწყობილობებზე?

პასუხი:

Login blocking აყოვნებს ან ბლოკავს შემდგომი ავტორიზაციის მცდელობებს გარკვეული რაოდენობის წარუმატებელი ლოგინების შემდეგ, რაც ხელს უშლის brute-force შეტევებს.

8. რისთვის გამოიყენება SSH კონფიგურაცია Cisco მოწყობილობებში?

პასუხი:

SSH უზრუნველყოფს დისტანციური მართვის სესიებს დაშიფრული არხის გამოყენებით, რაც იცავს ავტორიზაციის დეტალებს და მოწყობილობის მენეჯმენტს.

9. რატომ არის საჭირო privilege level-ების კონფიგურაცია?

პასუხი:

Privilege level-ების გამოყენება საშუალებას აძლევს ადმინისტრატორს გაანაწილოს მომხმარებლების უფლებები და მათზე მხოლოდ აუცილებელი ბრძანებები გააკეთოს ხელმისაწვდომი, უსაფრთხოების გაძლიერების მიზნით.

10. რა არის Role-Based CLI და რატომ ვიყენებთ მას?

პასუხი:

Role-Based CLI საშუალებას იძლევა გავყოთ ბრძანებების ჯგუფები სხვადასხვა როლისთვის (მაგალითად, WAN ინჟინერი და უსაფრთხოების ოპერატორი), რაც აუმჯობესებს მენეჯმენტს და ზრდის უსაფრთხოებას.

11. რატომ არის მნიშვნელოვანი IOS resilient configuration-ის ჩართვა?

პასუხი:

Resilient configuration ინახავს კრიტიკულ ფაილებს (IOS იმიჯი და კონფიგურაცია) სპეციალურ, დაცულ ადგილას მეხსიერებაში, რაც თავდასხმის ან მარცხის შემთხვევაში მოწყობილობის აღდგენას უზრუნველყოფს.

12. რა განსხვავებაა In-band და Out-of-band მენეჯმენტს შორის?

პასუხი:

In-band — მოწყობილობის მართვა ხდება იგივე ქსელით, რაც მომხმარებლების მონაცემებისთვის გამოიყენება.

Out-of-band — მართვისთვის გამოიყენება ცალკე კომუნიკაციის არხი, რაც მნიშვნელოვნად ზრდის უსაფრთხოებას.

13. როგორ მუშაობს Syslog და რატომ არის ის მნიშვნელოვანი?

პასუხი:

Syslog აგროვებს და აგზავნის ქსელური მოწყობილობების მიერ გენერირებულ შეტყობინებებს ცენტრალურ სერვერზე, რაც აუცილებელია მონიტორინგისთვის, ანალიზისთვის და ქსელური ინციდენტების დიაგნოსტიკისთვის.

14. რატომ არის SNMPv3 აუცილებელი SNMPv1 ან SNMPv2-ის ნაცვლად?

პასუხი:

SNMPv3 მხარს უჭერს ავთენტიფიკაციას და დაშიფვრას, რაც იცავს მართვის შეტყობინებებს სხვის მიერ წაკითხვისა და შეცვლისგან.

15. რატომ უნდა დაიყოს NTP-ის დროის წყაროები სექრეტული წყაროებიდან?

პასუხი:

სწორი დრო აუცილებელია ლოგების სინქრონიზაციისთვის და სერტიფიკატების მოქმედების ვადების სწორად მართვისთვის. სექრეტული წყაროებიდან (დაცული სერვერები) მიღებული დრო ამცირებს spoofed (გაყალბებული) დროის შეტევების რისკს.

16. როგორ მუშაობს AutoSecure ფუნქცია?

პასუხი:

AutoSecure ფუნქცია აწესრიგებს მოწყობილობაზე უსაფრთხოების კონფიგურაციას, დეაქტივირებს არასაჭირო სერვისებს და ახდენს საჭირო პარამეტრების ავტომატურ დაყენებას wizard-ის მეშვეობით.

17. რატომ არის Routing Protocol Authentication აუცილებელი OSPF-ში?

პასუხი:

Authentication იცავს როუტინგის ინფორმაციას არავარგისი მოწყობილობებისგან, ხელს უშლის როუტინგის ცხრილების მანიპულაციას და გარჩევას (routing table poisoning).

18. რა არის Control Plane Policing (CoPP) და როგორ იცავს ის მოწყობილობას?

პასუხი:

CoPP ფილტრავს და ლიმიტირებს იმ ტრაფიკს, რომელიც მიდის მოწყობილობის control plane-ზე (CPU-ზე), რაც იცავს რესურსების გადატვირთვისგან და ხელს უშლის მავნე შეტევებს.

19. რა საფრთხეებია დამახასიათებელი Layer 2 (Switch) ქსელისთვის?

პასუხი:

Layer 2 მოწყობილობები დაუცველია:

CAM Table Overflow შეტევების,

VLAN Hopping,

DHCP spoofing და starvation,

ARP spoofing/poisoning,

IP source spoofing,

STP manipulation შეტევების მიმართ.

20. რა არის CAM Table Overflow შეტევა და როგორ მოქმედებს ის?

პასუხი:

მტერი ავსებს switch-ის CAM table-ს ყალბი MAC მისამართებით, რის შედეგად switch იწყებს ყველა პაკეტის broadcast რეჟიმში გაგზავნას და თავდამსხმელს ეძლევა საშუალება მონაცემების ჩაჭრისთვის.

21. როგორ შეიძლება CAM Table შეტევისგან დაცვა?

პასუხი:

Port Security-ის ჩართვით:

მაქსიმალური MAC-ების რაოდენობის შეზღუდვა,

სტატიკური MAC მისამართების რეგისტრაცია,

Dynamic MAC address learning-ის კონტროლი.

22. რას ნიშნავს Port Security-ის Protect, Restrict და Shutdown რეჟიმები?

პასუხი:

Protect — ჩუმად წყვეტს დაუმტკიცებელ MAC-ის პაკეტებს.

Restrict — წყვეტს და აგზავნის log შეტყობინებას.

Shutdown — პორტს აყენებს "error-disabled" მდგომარეობაში.

23. როგორია Port Security Aging მექანიზმის მუშაობა?

პასუხი:

Port Security Aging ავტომატურად შლის MAC მისამართებს მითითებული დროის გასვლის შემდეგ, რაც ამცირებს ქსელის მართვის სირთულეს.

24. რატომ არის VLAN hopping შეტევა საშიში?

პასუხი:

VLAN hopping საშუალებას აძლევს თავდამსხმელს გადაკვეთოს VLAN ბარიერები და არაუფლებრივ VLAN-ებში მოხვდეს ან პაკეტები გადაიტანოს სხვაგან.

25. როგორ უნდა დავიცვათ ქსელი VLAN hopping-ისგან?

პასუხი:

ყველა არაპირველადი პორტი დავაყენოთ access mode-ზე.

დავუკეტოთ DTP (Dynamic Trunking Protocol).

გამოვიყენოთ ვალიდური Native VLAN-id-ები.

26. რა არის DHCP Spoofing შეტევა?

პასუხი:

თავდამსხმელი აწარმოებს ყალბ DHCP სერვერს და აძლევს შეცდომით მისამართებს (default gateway, DNS), რაც საშუალებას აძლევს შეაჩეროს ან გააკონტროლოს ტრაფიკი.

27. როგორ ვებრძოლოთ DHCP Spoofing შეტევას?

პასუხი:

DHCP Snooping-ის ჩართვით:

სანდო (trusted) და არასანდო (untrusted) პორტების განისაზღვრით.

ნებადართულია მხოლოდ სანდო პორტზე DHCP სერვერიდან გაგზავნილი შეტყობინებები.

28. რა ხდება DHCP Starvation შეტევისას?

პასუხი:

თავდამსხმელი ავსებს DHCP სერვერის მისამართების პულს ყალბი მოთხოვნებით (DISCOVER), რაც ამოწურავს IP მისამართებს და აჩერებს ლეგალურ კლიენტებს ქსელში დაკავშირებისგან.

29. როგორ მუშაობს ARP Spoofing შეტევა?

პასუხი:

თავდამსხმელი აგზავნის ყალბ ARP პასუხებს, აყალბებს MAC-IP ასოციაციას ქსელში, რაც საშუალებას აძლევს გადაიტანოს ტრაფიკი თავის მოწყობილობაზე.

30. როგორ ვიცავთ ქსელს ARP spoofing-ისგან?

პასუხი:

Dynamic ARP Inspection (DAI) გამოყენებით:

შედარება DHCP snooping binding table-თან.

დაუშვებელია დაუმტკიცებელი ARP შეტყობინებების გატარება.

31. რა არის IP Source Guard და როგორ მუშაობს?

პასუხი:

IP Source Guard ფiltrobs პაკეტებს:

შეზღუდავს IP და MAC მისამართის spoofing შეტევებს.

პაკეტი გაშვებულია მხოლოდ მაშინ, როდესაც შეესაბამება DHCP Snooping Binding Table-ს.

32. რა საფრთხეებია დაკავშირებული Spanning Tree Protocol-თან (STP)?

პასუხი:

თავდამსხმელმა შეიძლება გააგზავნოს ყალბი BPDU შეტყობინებები და დაინიშნოს Root Bridge-ად, რაც ქსელის გზების კონტროლს მისცემს.

33. როგორ უნდა დავიცვათ STP ინფრასტრუქტურა?

პასუხი:

BPDU Guard — აკრძალვა მომხმარებლის პორტებზე BPDU-ების მიღებაზე.

Root Guard — თავიდან აცილება Root Bridge-ის უნებართვო შეცვლის.

Loop Guard — ბლოკავს unidirectional ლინკებს.

PortFast — სწრაფი აქტივაცია End-Device პორტებისთვის.

34. რა ფუნქცია აქვს Private VLAN (PVLAN)-ს?

პასუხი:

PVLAN ხელს უშლის იმავე VLAN-ში მყოფ მოწყობილობებს ერთმანეთთან პირდაპირ კომუნიკაციაში ყოფნას, რაც ამცირებს თავდასხმის რისკებს.

35. როგორია DHCP Snooping-ის კონფიგურაციის ძირითადი ნაბიჯები?

პასუხი:

DHCP Snooping-ის აქტივაცია ვლანზე.

სანდო პორტების მონიშვნა.

სიჩქარის ლიმიტების დაყენება untrusted პორტებზე.

36. რას გულისხმობს VLAN Double-Tagging შეტევა?

პასუხი:

თავდამსხმელი ორ წარწერას (Tag) უმატებს Ethernet ჩარჩოს — Switch პირველი ტეგს აშორებს, მეორე კი რჩება, რაც საშუალებას აძლევს თავდამსხმელს სხვა VLAN-ში გადასვლას.

**Check Point კიბერუსაფრთხოების ადმინისტრირების გამოცდის სავარჯიშოები**

**სავარაუდო პასუხებიანი კითხვები (20)**

**1. რა არის Check Point-ის მთავარი მართვის კომპონენტი?**

A. Security Gateway B. SmartConsole C. Security Management Server D. Endpoint Security Client

**სწორი პასუხი: C. Security Management Server**

**2. რომელი პროტოკოლი გამოიყენება Check Point-ის კლიენტსა და Security Gateway-ს შორის VPN კავშირისთვის?**

A. PPTP B. L2TP C. SSL D. IPsec

**სწორი პასუხი: D. IPsec**

**3. Check Point-ის რომელი კომპონენტი უზრუნველყოფს მაღალ ხელმისაწვდომობას?**

A. SecureXL B. ClusterXL C. CoreXL D. SmartXL

**სწორი პასუხი: B. ClusterXL**

**4. რა არის SmartConsole?**

A. CLI ინტერფეისი Security Gateway-ისთვის B. გრაფიკული ინტერფეისი ადმინისტრატორებისთვის C. ლოგების ანალიზის ავტომატური ინსტრუმენტი D. სენსორი შეტევების აღმოსაჩენად

**სწორი პასუხი: B. გრაფიკული ინტერფეისი ადმინისტრატორებისთვის**

**5. რომელი კომანდა გამოიყენება Check Point-ის ფაირვოლის სტატუსის შესამოწმებლად?**

A. cpstat B. fw stat C. status fw D. firewall status

**სწორი პასუხი: B. fw stat**

**6. რას წარმოადგენს Software Blades Check Point-ის არქიტექტურაში?**

A. აპარატურულ კომპონენტებს B. მოდულურ ფუნქციონალურ კომპონენტებს C. ქსელის მონიტორინგის სკრიპტებს D. გარე აპლიკაციების API-ებს

**სწორი პასუხი: B. მოდულურ ფუნქციონალურ კომპონენტებს**

**7. რომელი ინსტრუმენტი გამოიყენება Check Point-ის სისტემის მონიტორინგისთვის რეალურ დროში?**

A. SmartView Tracker B. SmartLog C. SmartEvent D. SmartView Monitor

**სწორი პასუხი: D. SmartView Monitor**

**8. რომელი მოდული უზრუნველყოფს წარმადობის ოპტიმიზაციას Check Point-ის გადაწყვეტილებებში?**

A. SecureXL B. CheckXL C. FastXL D. TurboXL

**სწორი პასუხი: A. SecureXL**

**9. რა არის პირველი აუცილებელი ნაბიჯი Security Gateway-ის კონფიგურაციისას?**

A. VPN კონფიგურაცია B. ფაირვოლის წესების შექმნა C. ინტერფეისებისა და IP მისამართების კონფიგურაცია D. IPS პროფილების შექმნა

**სწორი პასუხი: C. ინტერფეისებისა და IP მისამართების კონფიგურაცია**

**10. რომელი ფუნქცია უზრუნველყოფს აპლიკაციების იდენტიფიკაციასა და კონტროლს?**

A. URL Filtering B. Application Control C. IPS D. Anti-Bot

**სწორი პასუხი: B. Application Control**

**11. რა არის SIC Check Point-ის კონტექსტში?**

A. Secure Internet Connection B. Security Information Center C. Secure Internal Communication D. System Integrity Check

**სწორი პასუხი: C. Secure Internal Communication**

**12. რომელი მახასიათებელი მიეკუთვნება Check Point Infinity არქიტექტურას?**

A. მხოლოდ ქსელის დაცვა B. მხოლოდ ენდპოინტების დაცვა C. ერთიანი უსაფრთხოების არქიტექტურა ყველა გარემოსთვის D. მხოლოდ ღრუბლოვანი სერვისების დაცვა

**სწორი პასუხი: C. ერთიანი უსაფრთხოების არქიტექტურა ყველა გარემოსთვის**

**13. რომელ ფაილში ინახება Security Gateway-ის ძირითადი კონფიგურაცია?**

A. config.xml B. objects.C C. database.mdb D. security.conf

**სწორი პასუხი: B. objects.C**

**14. რა მნიშვნელობა აქვს "hide" NAT-ს Check Point-ში?**

A. წყაროს მისამართის დამალვა ერთი საჯარო IP-ის უკან B. დანიშნულების მისამართის დამალვა C. პორტების გადამისამართება D. სერვისების დაბლოკვა

**სწორი პასუხი: A. წყაროს მისამართის დამალვა ერთი საჯარო IP-ის უკან**

**15. როგორ მუშაობს CoreXL ტექნოლოგია?**

A. ანაწილებს პაკეტებს სხვადასხვა ფიზიკურ ინტერფეისზე B. ანაწილებს პაკეტებს სხვადასხვა CPU ბირთვზე C. ამცირებს მეხსიერების გამოყენებას D. ზრდის დისკის I/O წარმადობას

**სწორი პასუხი: B. ანაწილებს პაკეტებს სხვადასხვა CPU ბირთვზე**

**16. რომელი ფუნქციონალი უზრუნველყოფს მავნე კოდის ამოღებას დოკუმენტებიდან?**

A. Threat Emulation B. Threat Extraction C. Anti-Virus D. Content Scanner

**სწორი პასუხი: B. Threat Extraction**

**17. რომელი ინფორმაცია არ არის წარმოდგენილი SmartLog-ის მთავარ ხედში?**

A. წყარო IP მისამართი B. დანიშნულების IP მისამართი C. CPU გამოყენება D. სერვისი

**სწორი პასუხი: C. CPU გამოყენება**

**18. რა არის Policy Installation-ის მთავარი მიზანი?**

A. ფაირვოლის წესების შექმნა B. წესების კომპილაცია და გავრცელება Security Gateway-ზე C. ლოგების შეგროვება D. კონფიგურაციის დაარქივება

**სწორი პასუხი: B. წესების კომპილაცია და გავრცელება Security Gateway-ზე**

**19. რა ინფორმაციას შეიცავს cpinfo გამომავალი ფაილი?**

A. მხოლოდ ქსელის კონფიგურაციას B. მხოლოდ ლიცენზიის ინფორმაციას C. დიაგნოსტიკის სრულ ინფორმაციას სისტემის შესახებ D. მხოლოდ ფაირვოლის წესებს

**სწორი პასუხი: C. დიაგნოსტიკის სრულ ინფორმაციას სისტემის შესახებ**

**20. რომელი check point-ის კომპონენტია პასუხისმგებელი მობილური კლიენტების VPN კავშირზე?**

A. Mobile Access Blade B. Endpoint Security C. Remote Access D. Site-to-Site VPN

**სწორი პასუხი: A. Mobile Access Blade**

**ღია კითხვები (5)**

**1. აღწერეთ Check Point-ის უსაფრთხოების არქიტექტურა და მისი ძირითადი კომპონენტები.**

**პასუხი:**

Check Point-ის უსაფრთხოების არქიტექტურა შედგება რამდენიმე მნიშვნელოვანი კომპონენტისგან, რომლებიც ერთობლივად უზრუნველყოფენ ქსელების, აპლიკაციებისა და მონაცემების კომპლექსურ დაცვას.

**ძირითადი კომპონენტები:**

1. **Security Management Server (SMS)** - ცენტრალიზებული მართვის სისტემა, რომელიც პასუხისმგებელია:
   * უსაფრთხოების პოლიტიკის შექმნაზე და მართვაზე
   * Gateway-ების კონფიგურაციაზე
   * ლოგების შეგროვებასა და ანალიზზე
   * ანგარიშგებაზე
2. **Security Gateway** - უსაფრთხოების გარემოს აღსრულების კომპონენტი, რომელიც უზრუნველყოფს:
   * ფაირვოლის ფუნქციონალს
   * ტრაფიკის ინსპექციას
   * VPN ფუნქციონალს
   * საფრთხეების პრევენციას
   * შეიძლება იყოს როგორც ფიზიკური, ასევე ვირტუალური ფორმით
3. **SmartConsole** - ადმინისტრატორის გრაფიკული ინტერფეისი, რომელიც გამოიყენება:
   * პოლიტიკების შესაქმნელად და დასადეპლოვებლად
   * ობიექტების სამართავად
   * ქსელის მონიტორინგისთვის
   * ტრაბლშუთინგისთვის
4. **Software Blades** - მოდულური კომპონენტები, რომლებიც უზრუნველყოფენ დამატებით ფუნქციონალს:
   * IPS (Intrusion Prevention System)
   * Application Control
   * URL Filtering
   * Anti-Bot და Anti-Virus
   * Identity Awareness
   * Mobile Access
   * DLP (Data Loss Prevention)
5. **Endpoint Security** - კლიენტების დაცვა, რომელიც მოიცავს:
   * SandBlast Agent
   * Full Disk Encryption
   * Media Encryption & Port Protection
   * Anti-Malware და Anti-Ransomware

არქიტექტურის დამატებითი მნიშვნელოვანი ასპექტები:

* **Multi-Domain Management** - რამდენიმე ლოგიკური დომენის მართვა ერთი Management Server-იდან
* **Provider-1** - მრავალტენანტიანი მართვის გადაწყვეტილება
* **SmartEvent** - უსაფრთხოების მოვლენების მონიტორინგი და ანალიზი
* **Check Point Infinity** - არქიტექტურული მიდგომა, რომელიც აერთიანებს ქსელის, ენდპოინტების, მობილურების და ღრუბლის უსაფრთხოებას ერთიან პლატფორმაში

ეს კომპონენტები ერთობლივად ქმნიან კომპლექსურ უსაფრთხოების ეკოსისტემას, რომელიც უზრუნველყოფს მრავალშრიან დაცვას (defense-in-depth) და საშუალებას აძლევს ორგანიზაციებს ეფექტურად გაუმკლავდნენ თანამედროვე კიბერსაფრთხეებს.

**2. როგორ მუშაობს Threat Prevention სისტემა Check Point-ში და რა კომპონენტებისგან შედგება ის?**

**პასუხი:**

Check Point-ის Threat Prevention სისტემა წარმოადგენს მრავალშრიან უსაფრთხოების გადაწყვეტილებას, რომელიც შექმნილია თანამედროვე საფრთხეების (Advanced Threats) გამოსავლენად და შესაჩერებლად.

**მუშაობის პრინციპი:**

Threat Prevention მუშაობს მრავალდონიანი დაცვის პრინციპით, სადაც თითოეული დონე ფოკუსირებულია საფრთხეების სხვადასხვა ასპექტზე. სისტემა იყენებს როგორც სიგნატურაზე დაფუძნებულ მეთოდებს, ასევე ქცევაზე და ჰეურისტიკაზე დაფუძნებულ ანალიზს საფრთხეების იდენტიფიცირებისთვის.

**ძირითადი კომპონენტები:**

1. **IPS (Intrusion Prevention System)**:
   * რეალურ დროში ტრაფიკის ინსპექცია
   * სიგნატურებზე და პროტოკოლის ანომალიებზე დაფუძნებული დეტექცია
   * კონფიგურირებადი პროტექციის პროფილები
   * პროაქტიული შეტევების პრევენცია
   * IPS ფუნქციონირებს პროტექცია პროფილების ბაზაზე, რომლებიც შეიცავენ სხვადასხვა პროტექციების (signatures) ჯგუფებს
2. **Anti-Virus**:
   * მალვეარების დეტექცია და პრევენცია
   * მრავალძრავიანი სკანირება
   * რეალურ დროში ფაილების შემოწმება
   * სიგნატურებზე დაფუძნებული დეტექცია
   * კონფიგურირებადი პოლიტიკები სხვადასხვა ტიპის ფაილებისთვის
3. **Anti-Bot**:
   * ბოტნეტ კომუნიკაციის იდენტიფიცირება და ბლოკირება
   * C&C (Command and Control) სერვერებთან კავშირის აღმოჩენა
   * ინფიცირებული მოწყობილობების იდენტიფიკაცია
   * DNS და HTTP/S ტრაფიკის ინსპექცია
   * ბოტის ქცევის ანალიზი
4. **Threat Emulation (Sandbox)**:
   * საეჭვო ფაილების იზოლირებულ გარემოში გაშვება და ანალიზი
   * თქვენი ქსელისთვის გაგზავნამდე ფაილების უსაფრთხოების შემოწმება
   * ქცევაზე დაფუძნებული ანალიზი
   * Zero-day საფრთხეების იდენტიფიკაცია
   * დეტალური ანგარიშების გენერირება
5. **Threat Extraction**:
   * პოტენციურად საშიში კონტენტის ამოღება დოკუმენტებიდან
   * დოკუმენტების კონვერტაცია უსაფრთხო ფორმატში
   * აქტიური კონტენტის (მაკროები, სკრიპტები) ამოღება
   * ორიგინალური ფაილების შენახვა მოგვიანებით წვდომისთვის
   * ფაილების მყისიერი მიწოდება მომხმარებლებისთვის უსაფრთხო ფორმით
6. **URL Filtering**:
   * ვებ-გვერდების კატეგორიზაცია და ფილტრაცია
   * მავნე URL-ების ბლოკირება
   * URL რეპუტაციის შეფასება
   * პოლიტიკების განსაზღვრა კატეგორიების მიხედვით
7. **Application Control**:
   * აპლიკაციების იდენტიფიკაცია და კონტროლი
   * დეტალური პოლიტიკების განსაზღვრა აპლიკაციების მიხედვით
   * აპლიკაციებთან დაკავშირებული რისკების მართვა

**პოლიტიკების მართვა:**

Threat Prevention-ის ყველა კომპონენტი იმართება ცენტრალიზებული Threat Prevention Policy-ის მეშვეობით, რომელიც საშუალებას იძლევა შეიქმნას:

* Threat Prevention პროფილები
* გამონაკლისები
* Custom Signatures
* შეტყობინებების წესები

**თავისებურებები:**

* ინფორმაციის გაცვლა ThreatCloud-თან - Check Point-ის გლობალურ საფრთხეების დაზვერვის ქსელთან
* რეალურ დროში განახლებები ახალი საფრთხეების შესახებ
* მაღალი წარმადობა მრავალბირთვიანი არქიტექტურის გამოყენებით
* ავტომატური მიტიგაცია გამოვლენილი საფრთხეების მიმართ

Threat Prevention-ის ყველა კომპონენტი ინტეგრირებულია ერთიან სისტემაში და მართვადია SmartConsole-ის მეშვეობით, რაც უზრუნველყოფს თანმიმდევრულ დაცვას და გამარტივებულ ადმინისტრირებას.

**3. აღწერეთ ClusterXL-ის მუშაობის პრინციპი და კონფიგურაციის ძირითადი ნაბიჯები.**

**პასუხი:**

**ClusterXL-ის მუშაობის პრინციპი**

ClusterXL არის Check Point-ის მაღალი ხელმისაწვდომობის და დატვირთვის განაწილების ტექნოლოგია, რომელიც უზრუნველყოფს Security Gateway-ების უწყვეტ მუშაობას აპარატურული და პროგრამული უზრუნველყოფის მწყობრიდან გამოსვლის შემთხვევაშიც კი.

**ClusterXL-ის მუშაობის რეჟიმები:**

1. **High Availability (HA)** - ამ რეჟიმში ერთი Gateway არის აქტიური და ამუშავებს მთელ ტრაფიკს, ხოლო სხვა Gateway(ები) არის მზადყოფნის რეჟიმში (Standby). თუ აქტიური Gateway გამოვა მწყობრიდან, ერთ-ერთი Standby Gateway გახდება აქტიური.
2. **Load Sharing** - ყველა Gateway არის აქტიური და ტრაფიკი ნაწილდება მათ შორის. თუ რომელიმე Gateway გამოვა მწყობრიდან, მისი დატვირთვა გადანაწილდება დარჩენილ Gateway-ებზე.
3. **Load Balancing (VMAC)** - Virtual MAC რეჟიმი, სადაც ერთი ვირტუალური MAC მისამართი გამოიყენება კლასტერის მიერ და ტრაფიკი ნაწილდება წინასწარ განსაზღვრული წესებით.

**სინქრონიზაციის მექანიზმები:**

1. **State Synchronization** - კონექციების მდგომარეობის სინქრონიზაცია Gateway-ებს შორის, რაც უზრუნველყოფს კავშირების შენარჩუნებას გადართვის შემთხვევაში.
2. **ClusterXL Sync** - პროტოკოლი, რომელსაც იყენებენ Gateway-ები კლასტერის სტატუსის შესახებ ინფორმაციის გასაცვლელად.
3. **Heartbeat** - პერიოდული შეტყობინებები, რომლებიც გაიგზავნება Gateway-ებს შორის მათი მდგომარეობის შესამოწმებლად.

**ClusterXL-ის კონფიგურაციის ძირითადი ნაბიჯები:**

1. **წინაპირობების შემოწმება:**
   * ყველა Gateway-ს უნდა ჰქონდეს იდენტური აპარატურა და პროგრამული უზრუნველყოფის ვერსია
   * SIC კავშირის დამყარება ყველა Gateway-სა და Management Server-ს შორის
   * ქსელის ინტერფეისების დაგეგმვა და კონფიგურაცია
2. **Cluster ობიექტის შექმნა SmartConsole-ში:**
   * Gateways & Servers -ში კლიკი New Cluster-ზე
   * კლასტერის სახელისა და IP მისამართების მითითება
   * მუშაობის რეჟიმის არჩევა (HA, Load Sharing, VMAC)
   * Cluster მემბრების დამატება
3. **ინტერფეისების კონფიგურაცია:**
   * Cluster ინტერფეისების განსაზღვრა (Cluster IP, ინდივიდუალური IP მისამართები)
   * Sync ინტერფეისის კონფიგურაცია
   * Monitored interfaces-ის განსაზღვრა
4. **Cluster პარამეტრების კონფიგურაცია:**
   * Sync პარამეტრები
   * Heartbeat ინტერვალის განსაზღვრა
   * Failover-ის დაყოვნების განსაზღვრა
   * მონიტორინგის პარამეტრები
5. **დამატებითი კონფიგურაცია:**
   * Sync დატვირთვის შემცირება (კონკრეტული კონექციებისთვის)
   * კრიტიკული სერვისების მონიტორინგის დამატება
   * ჩავარდნის რეაგირების სცენარების დაზუსტება
6. **პოლიტიკის ინსტალაცია:**
   * Cluster ობიექტზე პოლიტიკის ინსტალაცია
   * Gateway-ების რესტარტი (საჭიროების შემთხვევაში)
7. **ტესტირება და ვერიფიკაცია:**
   * მოწყობილობების ჩართვა/გამორთვა Failover-ის შესამოწმებლად
   * კონექციების შენარჩუნების ტესტირება
   * დატვირთვის ტესტირება

**ძირითადი CLI კომანდები მონიტორინგისა და ტრაბლშუთინგისთვის:**

* cphaprob stat - კლასტერის სტატუსის შემოწმება
* cphaprob -a if - ინტერფეისების მონიტორინგის სტატუსის შემოწმება
* cphaprob -ia list - კლასტერის წევრების სტატუსის შემოწმება
* fw ctl pstat - კონექციების სინქრონიზაციის სტატუსის შემოწმება
* fw tab -t connections -s - აქტიური კონექციების შემოწმება

ClusterXL წარმოადგენს კრიტიკულ კომპონენტს მაღალი ხელმისაწვდომობის Check Point უსაფრთხოების ინფრასტრუქტურაში, რომელიც უზრუნველყოფს სერვისების უწყვეტობას და ტრაფიკის ოპტიმალურ განაწილებას.

**4. რა არის პოლიტიკის ინსტალაცია Check Point-ში და როგორ ხდება მისი განხორციელება?**

**პასუხი:**

**რა არის პოლიტიკის ინსტალაცია**

პოლიტიკის ინსტალაცია Check Point-ში არის პროცესი, რომლის დროსაც უსაფრთხოების წესები და კონფიგურაცია, რომლებიც შეიქმნა და დაკონფიგურირდა SmartConsole-ში, კომპილირდება და გადაეცემა Security Gateway-ს. ეს არის კრიტიკული პროცესი, რადგან მხოლოდ პოლიტიკის ინსტალაციის შემდეგ შედის ძალაში დაკონფიგურირებული უსაფრთხოების წესები.

**პოლიტიკის კომპონენტები, რომლებიც ინსტალირდება:**

1. **Access Control Policy** - ფაირვოლის წესები (Firewall Rules)
2. **Threat Prevention Policy** - IPS, Anti-Virus, Anti-Bot და სხვა საფრთხეების პრევენციის წესები
3. **Data Security Policy** - DLP წესები
4. **Mobile Access Policy** - მობილური წვდომის წესები
5. **ქსელური ობიექტები** - ჰოსტები, ქსელები, სერვისები და