

## ტექნიკური მოთხოვნები

შემოთავაზებული აპარატურა უნდა გააჩნდეს შემდეგი ფუნქციონალი:

- პრივილეგირებული ანგარიშების მართვის ორგანიზება სასიცოცხლო ციკლის სრული ავტომატიზაციით;
- პაროლების ავტომატური შეცვლა მიღებული პოლიტიკის საფუძველზე;
- როლებზე დაფუძნებული პრივილეგირებული მომხმარებლის წვდომის კონტროლი კრიტიკულ რესურსებზე, ყველა რესურსის საიდუმლოების სრული კონტროლით ადმინისტრატორის მიერ განსაზღვრული ცენტრალური პოლიტიკის საფუძველზე;
- იერარქიული ნებართვების გაცემის სისტემის მეშვეობით;
- სარისკო ბრძანებების კონტროლის ფუნქცია;
- პრივილეგირებულ ანგარიშებზე აქტივობის მონიტორინგი მომხმარებლებისთვის, რომლებსაც აქვთ წვდომა უაღრესად მგრძნობიარე რესურსებზე;
- ყველა პრივილეგირებული ანგარიშის გამოყენების სრული აუდიტის თვალყურის დევნების ორგანიზებისთვის;
- უსაფრთხოების ინციდენტის შემთხვევაში ანგარიშის პრივილეგირებული გამოყენების შესახებ რეპორტის უზრუნველყოფა, სრული სესიის ვიდეო ჩანაწერები პრივილეგირებულ ანგარიშებში შესული მომხმარებლების ხედვის უზრუნველყოფა, კლავიატურისა და მაუსის მოვლენების მონიტორინგის ჩათვლით;
- სისტემა უნდა შეესაბამებოდეს ქვემოთ მოცემულ პარამეტრებს:
  1. სერვერულ რეკში დასამაგრებელი აპარატურა
  2. მინიმალური ლოკალური + დისტანციური მომხმარებლები – 50 ან მეტი
  3. მაქსიმალური მხარდაჭერილი მოთხოვნების რაოდენობა – 5000 ან მეტი
  4. მომხმარებლის მენეჯმენტი – ლოკალური, LDAP, RADIUS, SAML, MFA (ინტეგრაცია უკვე არსებულ FortiTOKEN-თან), როლების მართვა
  5. მოთხოვნის დამტკიცება – დამტკიცების პროფილი (3 დონიანი), განხილვა და დამტკიცება, შეტყობინების მოთხოვნა
  6. მონიტორინგი და ჩაწერა – მომხმარებლის მონიტორინგი, აქტიური სესიების მონიტორინგი, სესიის ჩაწერა
  7. გამშვებები - PuTTY, RDP, Web Launcher(HTTP, HTTPS), Web RDP, Web SFTP, Web SMB, Web SSH, Web VNC, WinSCP, Custom Launcher
  8. ვიდეო ჟურნალი – ჩაწერა და დათვალიერება
  9. RDP ბუფერის ფუნქციის დაბლოკვა
  10. Cisco Device მხარდაჭერა Auto-Enable on Native Launcher
  11. ჩაშენებული საცავი – 10 ტბ ან მეტი
  12. ელექტრომომარაგების რაოდენობა – 2 ან მეტი
  13. ინტერფეისების რაოდენობა Ethernet RJ45 1 გიგაბიტი – 4 ან მეტი
  14. ინტერფეისების რაოდენობა SFP 1 გიგაბიტი – 4 ან მეტი
  15. შაბლონი და წვდომა - - Unix SSH, Windows Domain Account, Template for Cisco Devices, Custom Template
  16. HA კლასტერინგის მხარდაჭერის მოთხოვნა – აქტიური-პასიური რეჟიმი
  17. გარე ჟურნალის კოლექტორთან/ლოგის ანალიზატორთან ინტეგრაციის ჩაშენებული ფუნქცია
  18. სრული გარანტიის პერიოდი (განახლება, ლიცენზიები, ტექნიკური მხარდაჭერა) – 3 წელი ან მეტი

## შესასრულებელი სამუშაოები

- ახალი აპარატურის ფიზიკური ინსტალაცია, დაკაბელება და მარკირება;
- ახალი აპარატურის პირველადი კონფიგურაცია, არსებულ ინფრასტრუქტურასთან ინტეგრაცია და Firmware-ების ბოლო სტაბილურ ვერსიამდე განახლება;
- IT პერსონალის ტრენინგი;

## მოთხოვნები მომწოდებლის მიმართ

- პრეტენდენტმა უნდა წარმოადგინოს შემოთავაზებული პროდუქტების მწარმოებლის ავტორიზაციის წერილი (MAF).
- პრეტენდენტმა უნდა წარმოადგინოს ინფორმაცია შემოთავაზებული პროდუქტების მწარმოებლის მინიმუმ ორი ავტორიზებული სერვის ცენტრის არსებობის შესახებ, საქართველოში.

## Technical requirements

The proposed hardware should have the following functionality:

- Organization of management of privileged accounts with complete automation of the life cycle;
- automatic change of passwords based on the accepted policy;
- role-based privileged user access control to critical resources, with complete control over the secrecy of all resources based on a central policy defined by the administrator;
- Through the system of issuing hierarchical permits;
- risk orders control function;
- Monitor activity on privileged accounts for users who have access to highly sensitive resources;
- To organize a full audit trail of the use of all privileged accounts;
- In the event of a security incident, providing a report on the privileged use of the account, providing full session video recordings of users logged into privileged accounts, including monitoring of keyboard and mouse events;
- The system must comply with the following parameters:
  1. Hardware to be attached to the server rack
  2. Minimum local + remote users – 50 or more
  3. Maximum number of supported requests – 5000 or more
  4. User management – local, LDAP, RADIUS, SAML, MFA (integration with existing FortiTOKEN), role management
  5. Request approval – approval profile (3 levels), review and approval, notification request
  6. Monitoring and recording – user monitoring, active session monitoring, session recording
  7. Launchers - PuTTY, RDP, Web Launcher(HTTP, HTTPS), Web RDP, Web SFTP, Web SMB, Web SSH, Web VNC, WinSCP, Custom Launcher
  8. Video log - recording and viewing
  9. Block RDP buffer function
  10. Cisco Device Support Auto-Enable on Native Launcher
  11. Built-in storage – 10 TB or more
  12. Number of power supplies – 2 or more
  13. Number of interfaces Ethernet RJ45 1 gigabit – 4 or more
  14. Number of interfaces SFP 1 gigabit – 4 or more
  15. Template and Access - - Unix SSH, Windows Domain Account, Template for Cisco Devices, Custom Template
  16. HA clustering support requirement – active-passive mode
  17. Built-in integration with external log collector/log analyzer
  18. Full warranty period (update, licenses, technical support) – 3 years or more

## Work to be done

- physical installation, wiring and labeling of new hardware;

- Initial configuration of new hardware, integration with existing infrastructure and firmware update to the latest stable version;
- IT staff training;

#### Requirements for the supplier

- Bidder must submit a letter of authorization (MAF) from the manufacturer of the proposed products.
- The bidder must provide information on the existence of at least two authorized service centers of the manufacturer of the proposed products in Georgia.