EFFECTIVE CUTTING-EDGE SECURITY FOR A PUBLIC ELECTRIC UTILITY COMPANY- CASE STUDY FORTINET AND EPBIH

Adnan Švraka, Expert associate for maintenance of ICT equipment, EPBiH

ABOUT THE COMPANY

- Elektroprivreda BiH (Public Enterprise Electric Utility of Bosnia and Herzegovina) is the largest Electric Utility Company whose activities include:
  - Generation and distribution of electricity
  - Supply of electricity
  - Trading of electricity
  - Export and import of electricity, including the management of electricity system

MOTIVATION

- Equipment was near the end of its lifecycle
- Need for Highly Available solution to protect our crucial applications
- Provide secure connectivity to our remote locations through the internet
- Solution that could be managed from a single location
- Increased volume of SSL traffic
  - 50% currently with growth tendencies up to 75% by 2019

OBSOLESCENCE OF THE MULTI-VENDOR SECURITY APPROACH

- Multi vendor security solutions:
  - Cisco ASA 5540
  - Cisco IPS
  - Microsoft Forefront TMG
- Difficult to manage all the equipment
- No correlation

SECURITY CHALLENGE

- Complex internal network (many routing protocols)
- Remote locations needed a backup link through Internet
- Allow partner companies access to specific servers in companies IT infrastructure using SSL VPN
- Protection of company users
- Securing the communication between our company and other companies that we provide IT services to
- Minimize downtime

SECURITY FEATURES

- IPS
- Application control
- Web filtering
- Anti-Spam
- SSL inspection
- Reverse proxy
- Reporting

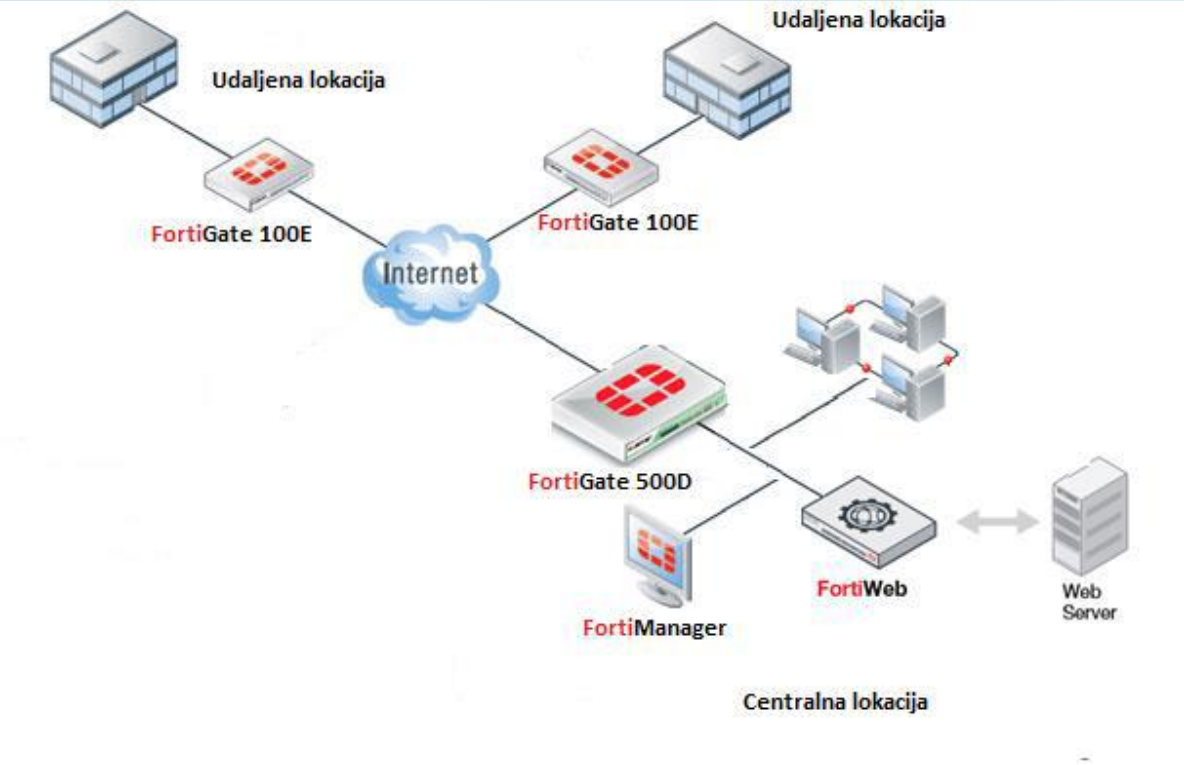
FORTINET FEATURES/ADVANTAGES

- Price
- Gartner leaders quadrant
- Easy to configure
- Easy to maintain and centrally monitor the system after the implementation
- User friendly interface

DEPLOYMENT

- FortiGate
- FortiWeb
- FortiManager
- FortiAnalyzer

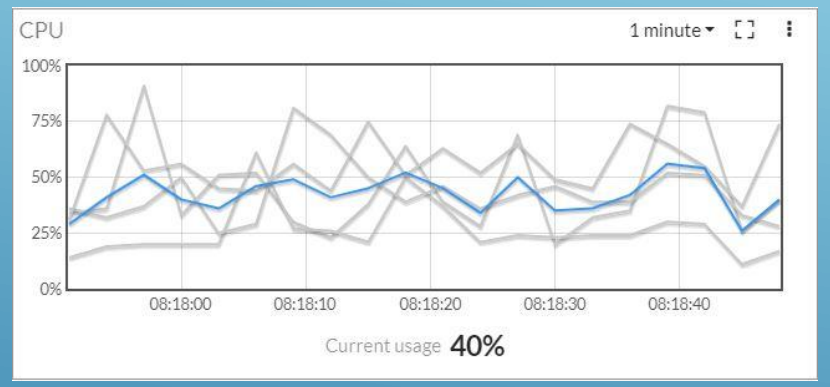
FORTINET IMPLEMENTATION

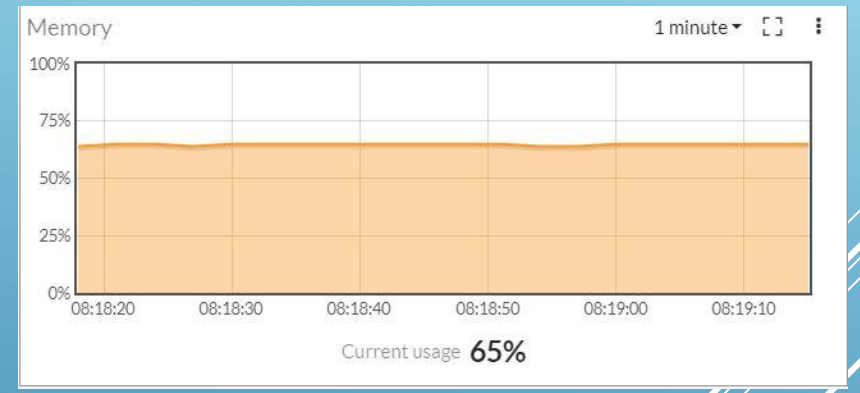


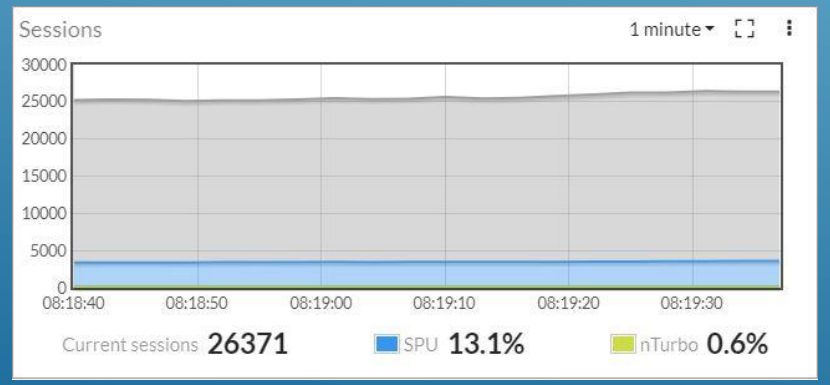
- Fortigate 500D
  - Firewall
  - VPN
  - Identity Awareness
  - Intrusion Prevention System (IPS)
  - URL Filtering
  - Application Control
  - Anti-Virus
  - Anti-Bot

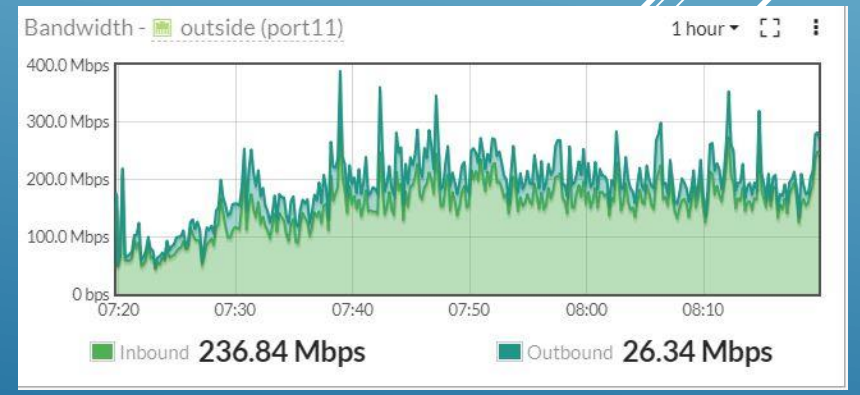
FORTINET IMPLEMENTATION- FORTIGATE 500D

- Throughput 350 Mbps
- 2000 users
- 50000 simultaneous sessions
- Full load

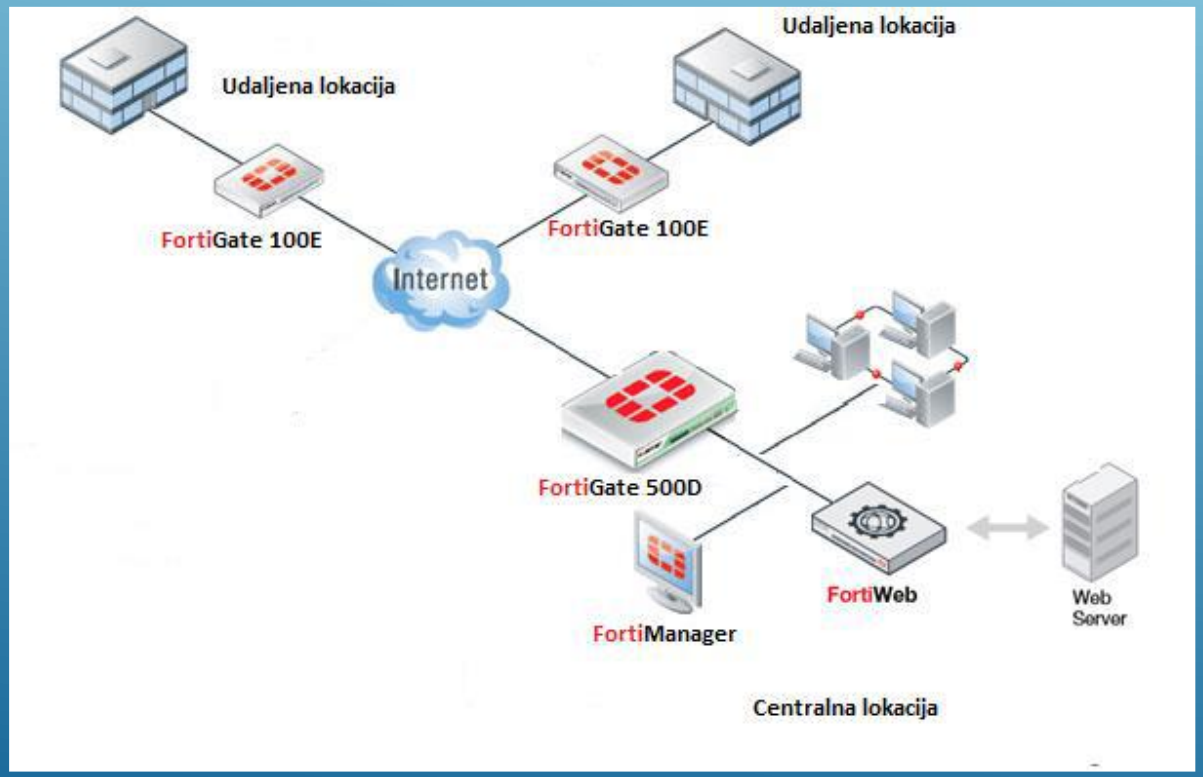








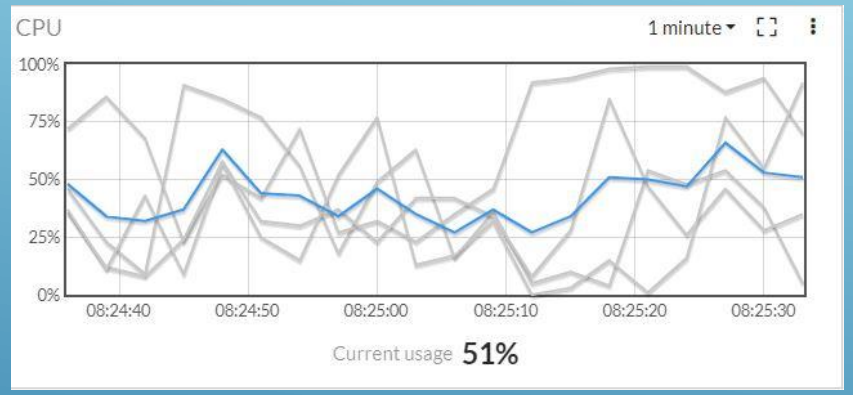
FORTINET IMPLEMENTATION

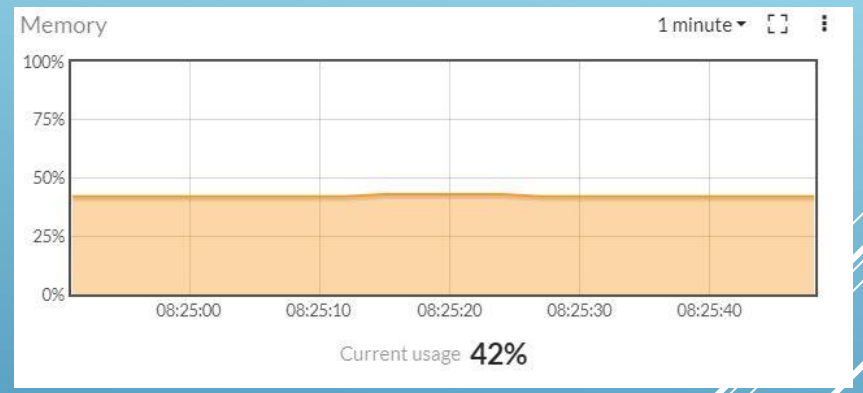


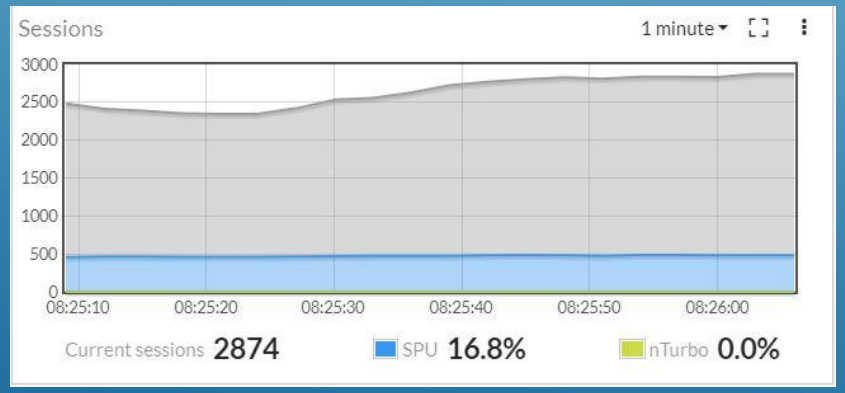
- Fortigate 100E
  - Firewall
  - VPN
  - Identity Awareness
  - Intrusion Prevention System (IPS)
  - URL Filtering
  - Application Control
  - Anti-Virus
  - Anti-Bot

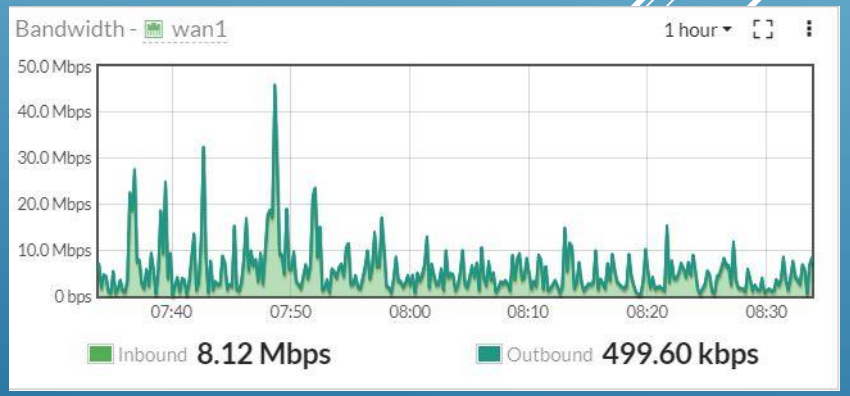
FORTINET IMPLEMENTATION – FORTIGATE 100E

- Throughput 100 Mbps
- 250 users
- 5000 simultaneous sessions
- Full load

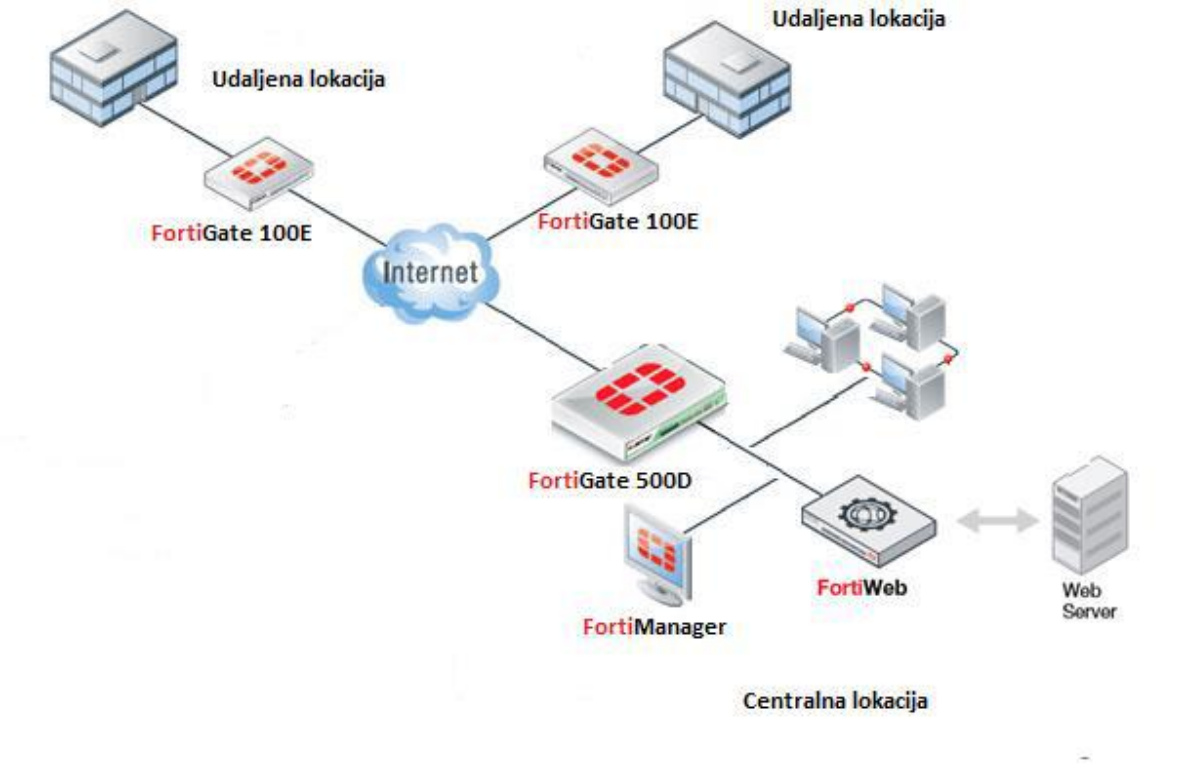




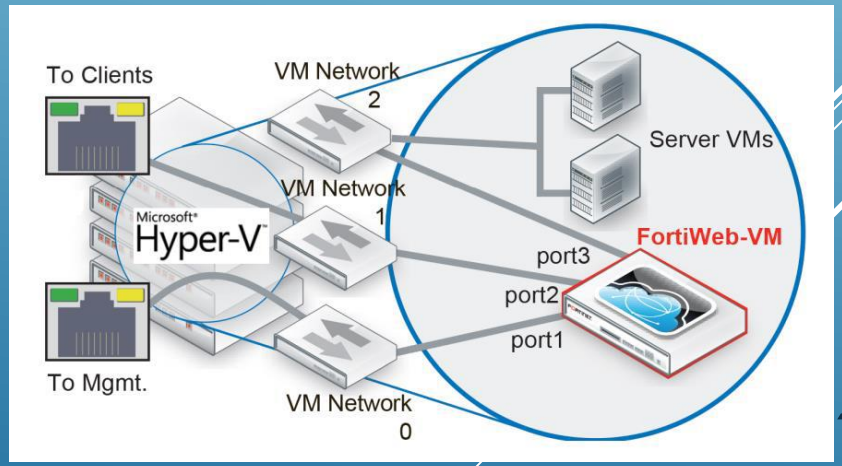




FORTINET IMPLEMENTATION

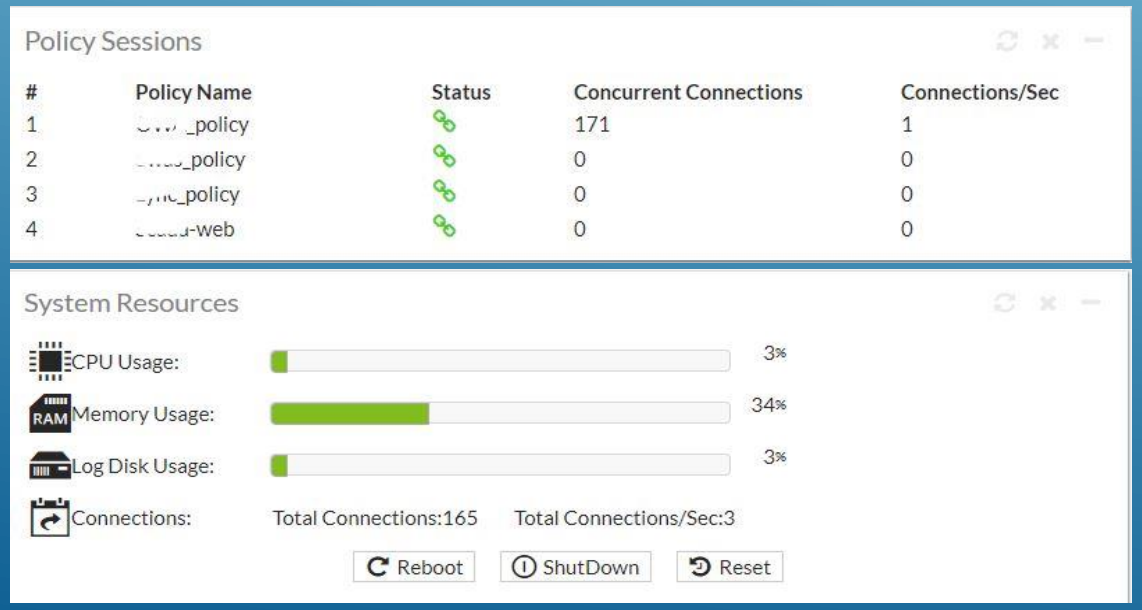


- Fortiweb
  - WAF
  - OWA

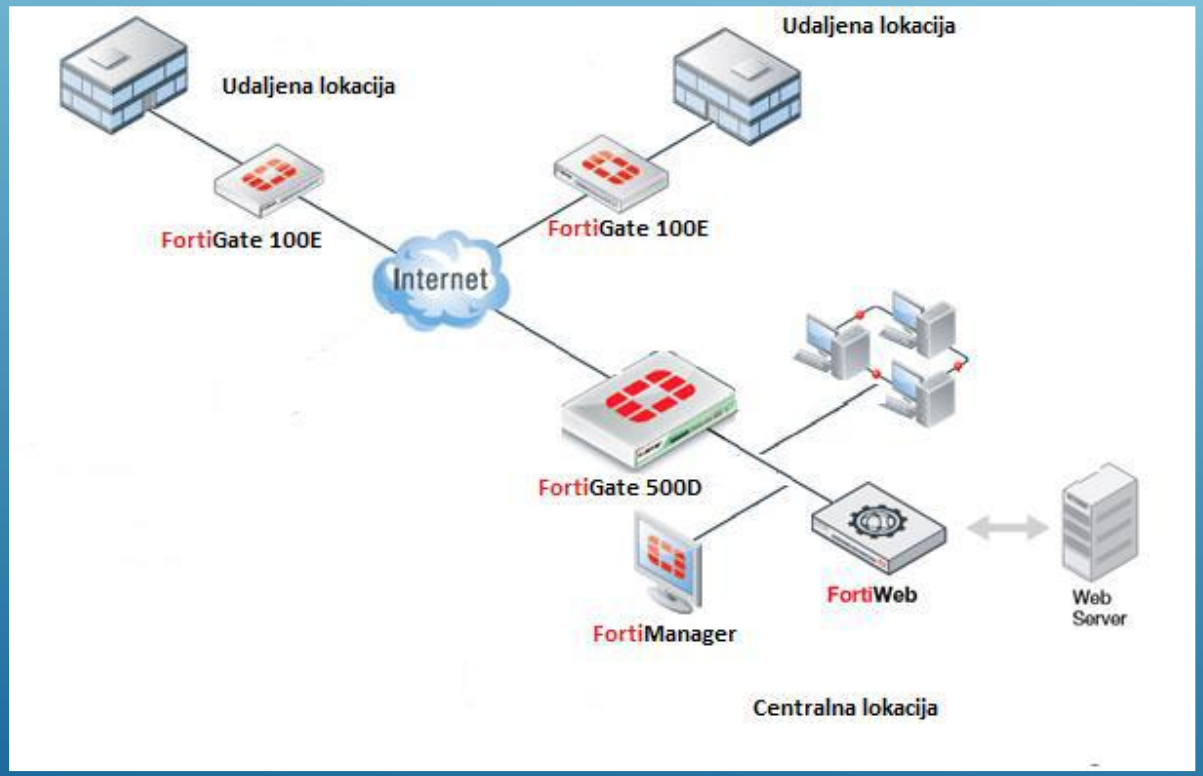


FORTINET IMPLEMENTATION - FORTIWEB

- Reverse proxy mode
- WAF
- Throughput 25 Mbps



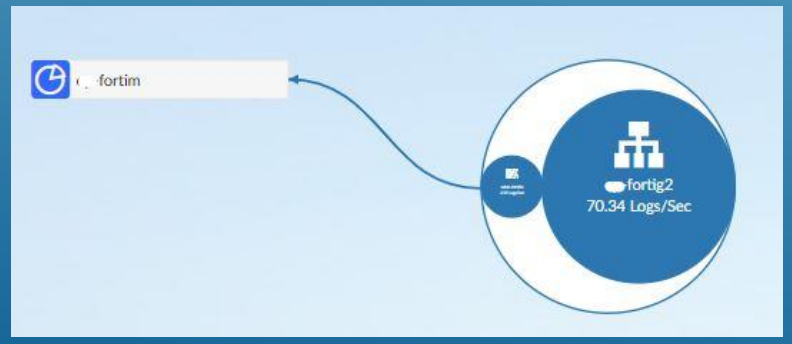
FORTINET IMPLEMENTATION

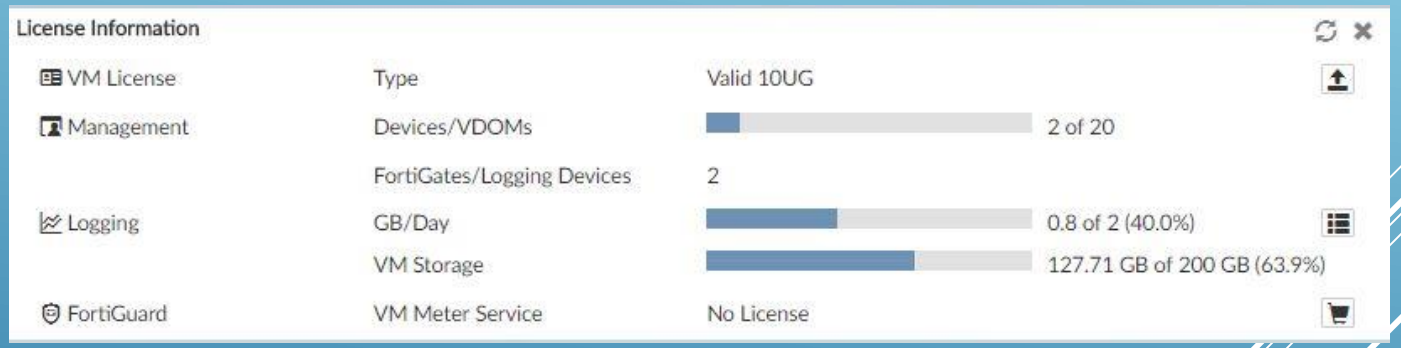


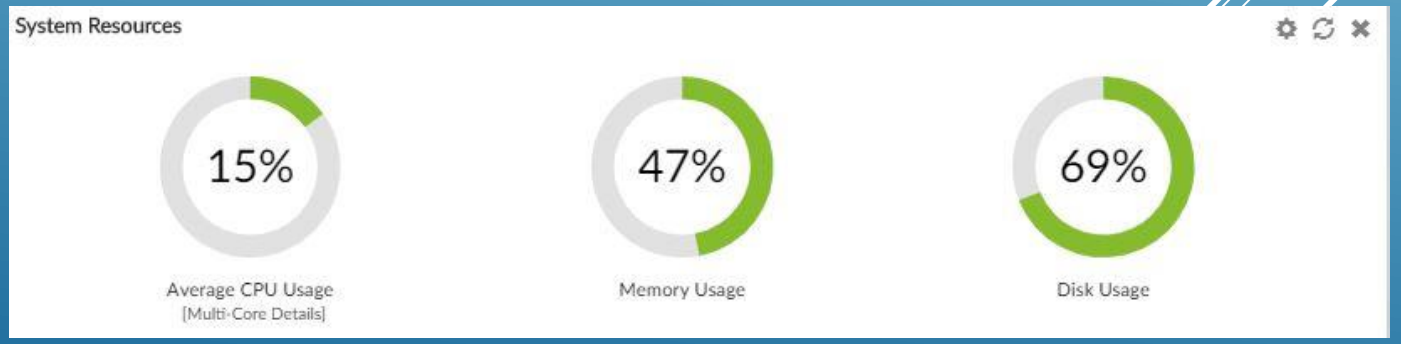
- FortiManager
  - Security Fabric
  - Configuration revision control and tracking
  - Centralized management
  - Administrative domains
  - Local FortiGuard service provisioning
  - Firmware management
  - Scripting
  - Logging and reporting
  - Fortinet device life cycle management

FORTINET IMPLEMENTATION - FORTIMANAGER

- 2 GB of logs daily
- Network profiling
- Managing whole fabric







FORTINET IMPLEMENTATION - OVERCOMING A CRITICAL SITUATION

- Disaster at the beginning of the implementation
- 3 days to production
- 7 days internet traffic re-routed
- 30 days for the whole implementation

BUSINESS BENEFITS

- Optimized infrastructure
- Increased IT security, management and control
- Reduced complexity resulting from multiple networking solutions in place
- Less maintenance time
- No downtime
- Management done by smaller team

VALUE OF PERFORMANCE AND SIMPLICITY

- 2500 users protected
- Internet access from multiple locations
- New threats found and remediated
- New solutions to be implemented
- Decreased number of security incidents
- Correlation
- Excellent reporting

CONCLUSION

- Gartner leaders quadrant
- User friendly and easy to implement
- All in one security appliance
- The most affordable security solution

QUESTIONS?