solutions 4networks
www.s4nets.com

Azure Networking and Security Appliance

Workshop | 10 days | $12,000

Offer:

The workshop will consist of an evaluation of your current network security firewalls with the intention to plan to migrate Cisco/Palo/etc. to the cloud.

Organizations have many types of firewalls in their environment and the s4nets team will develop a cost-effective plan to BYOL or subscribe to the appropriate appliances while maintaining a similar management plane across your datacenter and cloud environments.

The deliverables include a comprehensive plan to deploy and integrate next gen firewalls in the Azure environment while providing cost analysis documentation.

3 Phases

Discovery Phase

- Inventory existing network security firewalls and subscriptions, as well as management tools.
- Gather information on use case scenarios, rules and policies, and third-party connectors.
- Understand strategic goals, business objectives, and relevant security requirements.
- Discuss user experience and access policies.

Design and Documentation Phase

- Understand the Azure Infrastructure-Architecture, Assets, and RPO/RTO.
- Design appropriate NGFW environment based on sizing and performance objectives.
- Develop policies and rules migration strategy, where applicable.
- Estimate the spend for Azure and the NGFW platform.

Deployment Phase*

- Configure and roll-out the VM NGFW in Azure (with or without HA).
- Deploy all rules and policies agreed upon in the Design and Documentation Phase.
- Deploy existing or new Azure IaaS or Paas for the VM NGFW.
- Monitor the performance of the VM NGFW in Azure tenant, with consideration for replication if HA.
- Conduct DR test prior to hand-off to the client.

*Hours and cost based upon environment

What will a Next Gen firewall in the cloud provide me?

- Increased visibility within virtualized infrastructure monitoring
- Centralized management
- Identify and control applications, grant access based on users, and prevent known and unknown threats.
- Flexible licensing options
- Segment mission-critical applications and data using Zero Trust principles to improve security posture and achieve compliance.
- Rapid deployment capability
- Size and scale based on immediate needs
- Streamline workflow automation to ensure that security keeps pace with the rate of change in your cloud.
- QoS: Policy-based traffic shaping (priority, guaranteed, maximum) per application, per user, per tunnel, based on DSCP classification
- SSL termination with Deep Packet Inspection to identify known threats
- Traffic filtering rules by target URI

Contact:
Amanda Heinzman
aheinzman@s4nets.com
+1 (412) 626-3523