Handling DRP security appliances

Security architecture · https://nuabee.com/documents/handling-appliances-security-drp-nuabee/

Introduction

As part of its Disaster Recovery Plan (DRP) offering, Nuabee places particular emphasis on security, providing security appliances to meet specific customer needs.

Among the solutions available, Nuabee offers the **OPNsense** appliance, an open-source network security platform that can be deployed when needed.

Providing an OPNsense appliance

The OPNsense appliance is designed to cover a wide range of security needs in the DRP environment.

It can be used for :

1. **Firewall and Access Control**: Protect internal networks against unauthorized access and control incoming and outgoing traffic.
2. **Virtual Private Network (VPN)**: Facilitate secure connections between cloud and on-premises environments, ensuring that data in transit is encrypted and protected.
3. **Intrusion Detection and Prevention (IDS/IPS)**: Monitor network traffic to identify and block potential threats in real time.
4. **Content Filtering and Bandwidth Management**: Manage bandwidth usage and filter content to ensure optimal and secure use of network resources.

This appliance can be rapidly provisioned in the DRP space to ensure security continuity during disaster recovery. Nuabee has the expertise to help you define the right options for using OPNsense.

Support for other security appliances

In addition to OPNsense, it is possible to provision other KVM-compatible security appliances (hypervisors available in the OTC Cloud), depending on the customer's specific needs.

These appliances may include advanced firewall solutions, threat detection appliances, WAFs or other specialized security systems.

The process for deploying one of these appliances is as follows:

1. **Appliance provisioning**: A security appliance is provisioned in the PRA space according to the customer's specifications and requirements.
2. **Customer configuration**: Customers can configure the appliance according to their own security policies and operational requirements. This may include installing specific firewall rules, configuring VPNs, setting up IDS/IPS systems, and other customized security parameters.
3. **Creating a Configured Appliance Image**: Once the appliance has been configured, an image of this configuration is created. This image becomes a reference that can be restored at any time, ensuring that the security appliance is ready for operation in the event of a disaster.
4. **Disaster recovery**: In the event of a disaster, the configured appliance image can be quickly restored, ensuring that all critical security configurations are in place without delay. This enables rapid and secure resumption of operations, while minimizing service interruptions.

This process enables customers to maintain a high level of security even in the event of disaster recovery, with security appliances configured to their specific needs. By providing a flexible and adaptable solution, Nuabee ensures that businesses can focus on recovering from disasters with confidence, knowing that their security infrastructure is well managed and protected.

List of KVM-compatible security appliances (non-exhaustive list)

Brand	Name	Version tested	Comment / Process
Fortinet	FortiGate	6.4 / 7.0 / 7.2 / 7.4 / 7.6	Ability to use CloudInit to pass parameters to appliance instantiation
Sophos	XG	17.0	
Stormshield	UTM	3.11.8	Access to the administration interface fails if SSL or proxy filtering is in place (systematic disconnection otherwise). You must connect to a network that does not use http / https proxies to enable login.

PaloAlto	PAN-OS	8.0.0	
Cisco	ASAv	9.7.1	
Clavister	cOS Core	13.00.11.0.3	
Check Point	CloudGuard	R81	
Pulse Secure	PSA	9.1R11.4	
Sonicwall	NSv 200	6.5.0.2	License based on appliance MAC address (bad practice for use in the Cloud). Please contact your distributor for test and disaster recovery licenses.

Please contact us for a more complete version of this list.

Security appliance license management

In the case of most security appliances, such as **FortiGate, Palo Alto, Stormshield** or similar solutions, the license required to use these systems must be provided by the customer.

This includes licenses for advanced firewall functionality, threat detection systems, or any other specialized security modules that the customer wishes to deploy in the DRP space.

Nuabee does not provide the licenses for these appliances, and the customer must manage this with their security partner, but ensures that the infrastructure is ready to accommodate and integrate them effectively within the disaster recovery framework.

Conclusion

In conclusion, Nuabee can provide complementary security solutions in its Disaster Recovery Plan (DRP) spaces.

By offering security appliances such as OPNsense and enabling provisioning of other compatible solutions, such as FortiGate, Stormshield, Palo Alto, ..., Nuabee ensures efficient protection of cloud infrastructures. Customers benefit from a secure infrastructure, tailored to their specific needs and capable of responding rapidly in the event of a disaster.