FORCEPOINT
POWERED BY Raytheon

Solution Brief

Forcepoint Next Generation Firewall with Amazon Web Services (AWS)

FORCEPOINT SECURITY FOR PUBLIC CLOUD ENVIRONMENTS

Cloud-based services and virtual deployments are transforming businesses of all shapes and sizes. Traditional physical appliances and servers are rapidly disappearing because organizations need greater efficiency, agility and cost control to stay competitive. This widespread adaptation of cloud architectures puts added responsibility on security professionals and IT leaders to ensure that these new environments are just as secure as their physical predecessors.

Forcepoint Next Generation Firewall (NGFW) software-based solutions are uniquely designed to deliver maximum security with minimum cost and complexity. The Forcepoint NGFW Security Management Center (SMC) is a unified platform that gives you unmatched visibility, control and consistent policy enforcement to ensure regulatory compliance in physical infrastructure as well as virtual and cloud environments.

AWS CLOUD SECURITY

To secure cloud environments, Forcepoint brings leading next-generation firewall technology to Amazon Web Services (AWS) with proven scalability, operational efficiency and strong security. Easily and safely extend your organization's network – from data centers and network edge through your branch offices and remote sites – into your AWS cloud environment via a secure Virtual Private Network (VPN) gateway. Our centralized management enables you to create and deploy policies swiftly and consistently across all of your systems and quickly zero in on what's happening in both your AWS environment and your physical network.

MAXIMUM SECURITY, MINIMUM COMPLEXITY

The software-based architecture of Forcepoint's security for solutions such as advanced threat protection, deep packet inspection, and application-level control is designed for easy deployment to ensure maximum security without all the complexity and additional costs. The software-based Forcepoint security platform provides a comprehensive and integrated, defense-in-depth protection that can be tailored to the specific needs of each person, place or asset including firewall, VPN, IPS, URL filtering protection. This software platform offers all the existing capabilities in hardware-based appliances, including stateful inspection, granular policy and access control and redundant ISP connections – but without the box.

REAL-TIME VISIBILITY AND CONTROL

Forcepoint NGFW delivers complete visibility and control over the traffic flow within the virtual as well as cloud environment that traditional management consoles can't. The SMC provides rapid reporting on the amount of traffic passing between virtual systems and alerts administrators if a system is about to go down. Manage any number or combination of physical or virtual Forcepoint devices or clusters as well as software-based versions running on standard x86-hardware. The SMC also enhances virtual system security via a holistic monitoring dashboard with full stack application visibility and granular control.

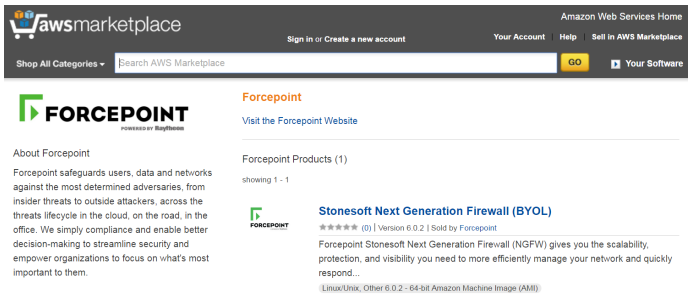
ENSURE REGULATORY COMPLIANCE

Maintaining compliance with the latest regulatory requirements such as PCI DSS, HIPAA, Sarbanes-Oxley and FISMA in the physical world is difficult, but remaining compliant in the virtual world is even more challenging. Traditional controls around each application are not present in a virtual environment. This makes determining which information was accessed by whom and when, impossible and is likely to raise a red flag with auditors.

The SMC gives you the level of monitoring, analysis and reporting you need to ensure compliance across virtual and physical networks. It gathers comprehensive data on all network events and presents them in clear and easily read audit logs. The SMC also lists security settings, reports system changes and provides the accurate audit reports you need, all at the press of a button.

QUICK AND ELASTIC DEPLOYMENT

To quickly deploy Forcepoint software-based architecture security in your AWS environment, simply choose one of the available options in the AWS Marketplace.



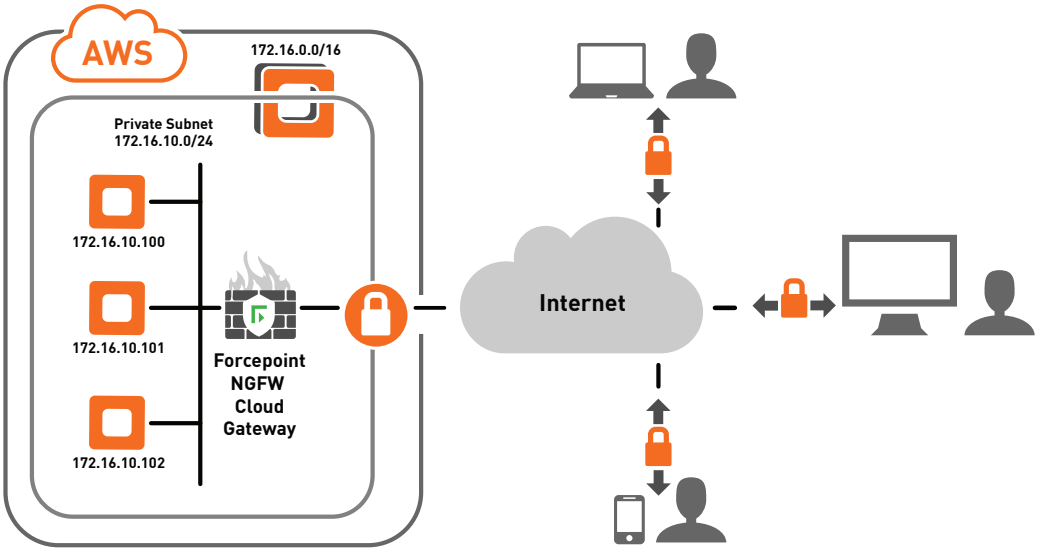
https://aws.amazon.com/marketplace/seller-profile?id=e67b339b-74fb-4353-a70f-93807f6550da

FORCEPOINT–AWS CLOUD CONNECTIVITY SOLUTIONS

How Forcepoint NGFW can be used with AWS cloud environments:

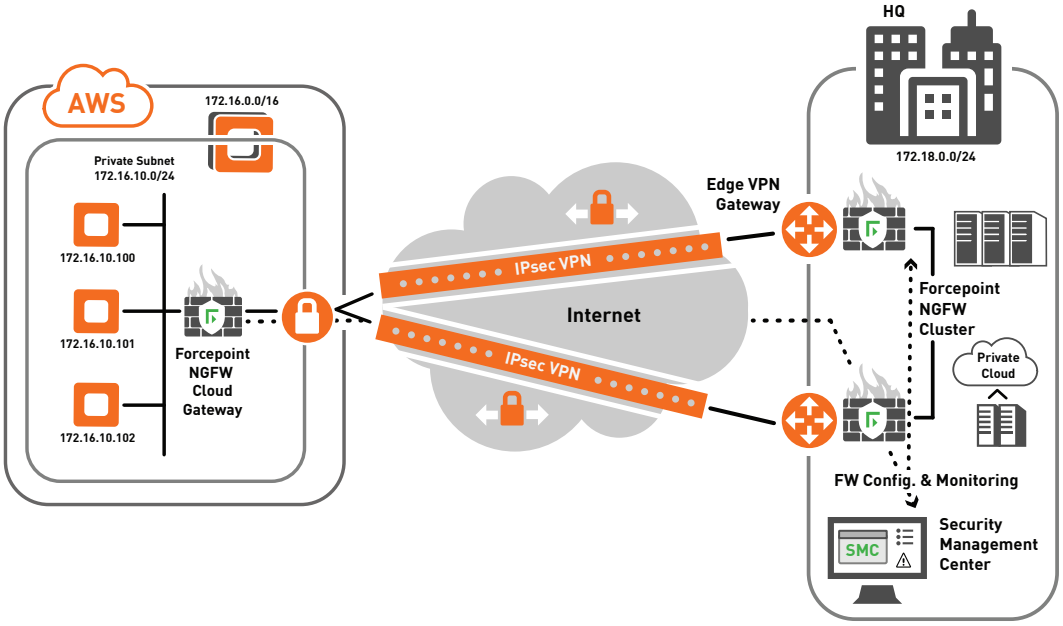
REMOTE ACCESS CONNECTIVITY

Securing remote access to the Amazon Cloud is a huge challenge for organizations. Forcepoint NGFW can be used as a cloud edge gateway to connect your remote users to Amazon Virtual Private Cloud (VPC). The Forcepoint NGFW cloud gateway can be deployed in an Amazon Elastic Compute Cloud (EC2) instance, offering advanced firewall features such as application awareness and user identity capabilities to protect your EC2 instances for all inbound and outbound access.



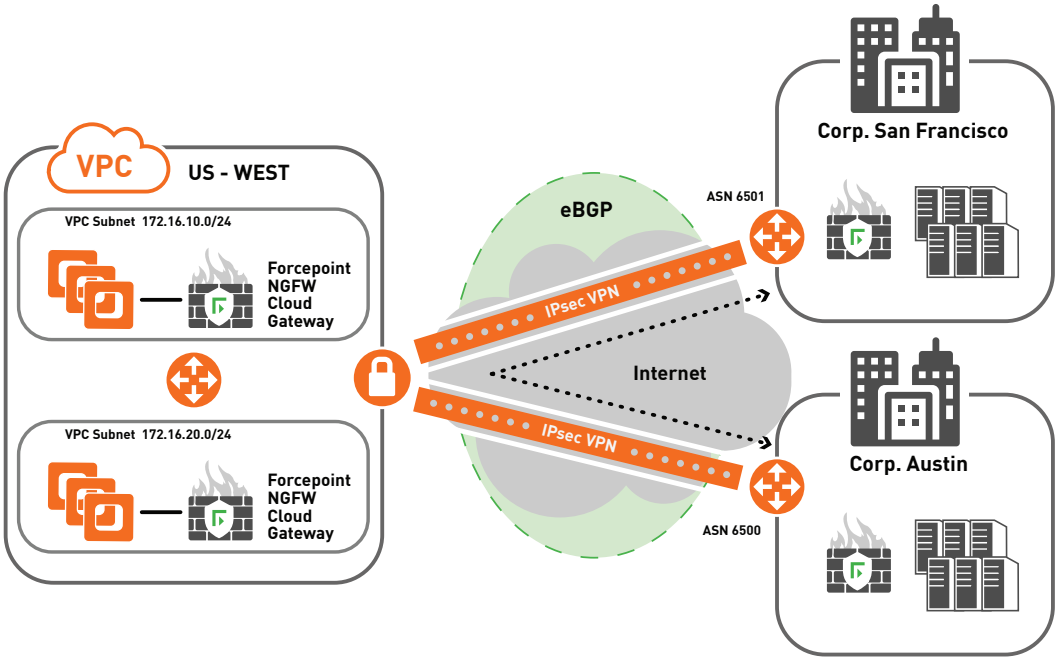
CORPORATE DATA CENTER CONNECTIVITY

Forcepoint NGFW physical and virtual gateways securely connect your corporate on-premise data centers to your virtual ones in AWS VPCs. Simply create one or more VPN connection between your data center network and your Forcepoint software VPN appliance running in your Amazon VPC network. Manage and control all your Forcepoint firewalls – software and physical – at both ends of the VPN connections via the SMC. You can also use a cluster of physical firewalls for the purpose of failover for business continuity on your headquarter side of the VPN connection.



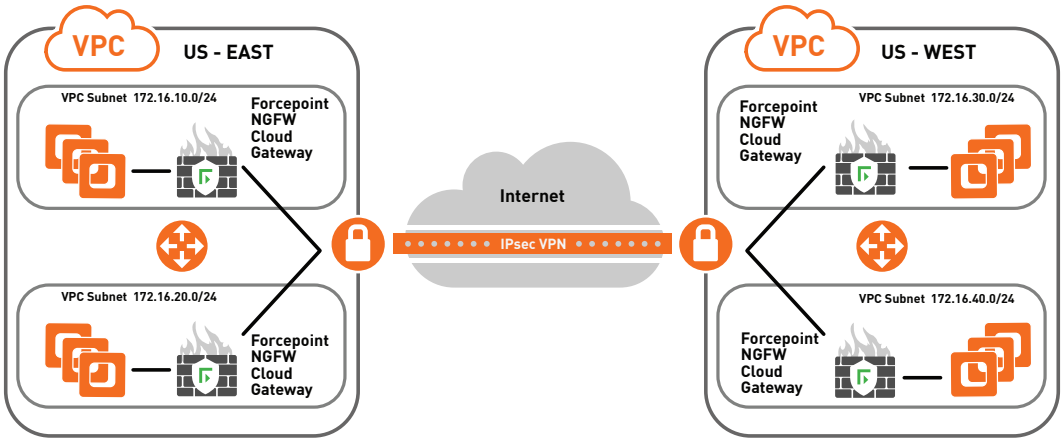
VPN CLOUDHUB

Securely connect remote branch offices using the AWS VPN CloudHub, operating on a simple hub-and-spoke model, for primary and backup connectivity between remote offices. Each remote site must have a unique ASN in order to send data to, and receive data from, the other site. The choice between using a static routing versus a dynamic routing for your VPN connections depends on how you want to handle failover. Both static and dynamic connectivity types technically use IPSEC to encapsulate security. Dynamic routing leverages BGP peering to exchange routes, and routing priorities between AWS and the remote endpoints is more flexible in that AWS will automatically change a BGP gateway route when/if their gateway changes.



INTERREGIONAL VPC-TO-VPC ROUTING

Create secure VPN tunnels between two or more Forcepoint software VPN appliances to connect VPCs across multiple AWS regions. You can manage, control and enforce security policies at both ends of the VPN connection using the Forcepoint Security Management tool.



CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[SOLUTION_BRIEF_FORCEPOINT_NGFW_AWS_EN] 700002.032917