FORCEPOINT
POWERED BY Raytheon

Solution Brief

FORCEPOINT Next Generation Firewall with Microsoft Azure

Forcepoint security for public cloud environments

Traditional physical appliances and servers are rapidly disappearing because organizations need greater efficiency, agility and cost control to stay competitive. Cloud-based services and virtual deployments are transforming these organizations; however, this widespread adaptation of cloud architectures puts added responsibility on security professionals and IT leaders to ensure 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. 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 in virtual and cloud environments.

Azure cloud security

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

Maximum security, minimum complexity

Forcepoint's software-based security architecture is designed for easy deployment to ensure maximum security without additional complexity and costs. This platform provides comprehensive, integrated, "defense-in-depth" protection that can be tailored to the specific needs of each person, place or asset (e.g., firewall, VPN, IPS, URL filtering protection). It offers all the existing capabilities in hardware-based appliances — stateful inspection, granular policy and access control, and redundant ISP connections — without the box.

Real-time visibility and control

Forcepoint SMC delivers complete visibility and control over the traffic flow within virtual and cloud environments, something traditional management consoles cannot do. It provides rapid reporting on the amount of traffic passing between virtual systems and alerts administrators if a system is about to go down. With Forcepoint SMC, you can manage any number of physical or virtual Forcepoint devices or clusters, as well as software-based versions running on standard x86-hardware. It 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 (e.g., PCI DSS, HIPAA, Sarbanes-Oxley, FISMA) in the physical world is difficult; it's even more so in the virtual world. Traditional controls around each application are not present in a virtual environment, which makes it impossible to determine what information was accessed by whom and when it was accessed. This lack of clarity is likely to raise a red flag with auditors.

Forcepoint 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. Forcepoint SMC also lists security settings, reports system changes and provides accurate audit reports, all at the press of a button.

Forcepoint – azure cloud connectivity solutions

Forcepoint NGFW can be used with Azure cloud environments.

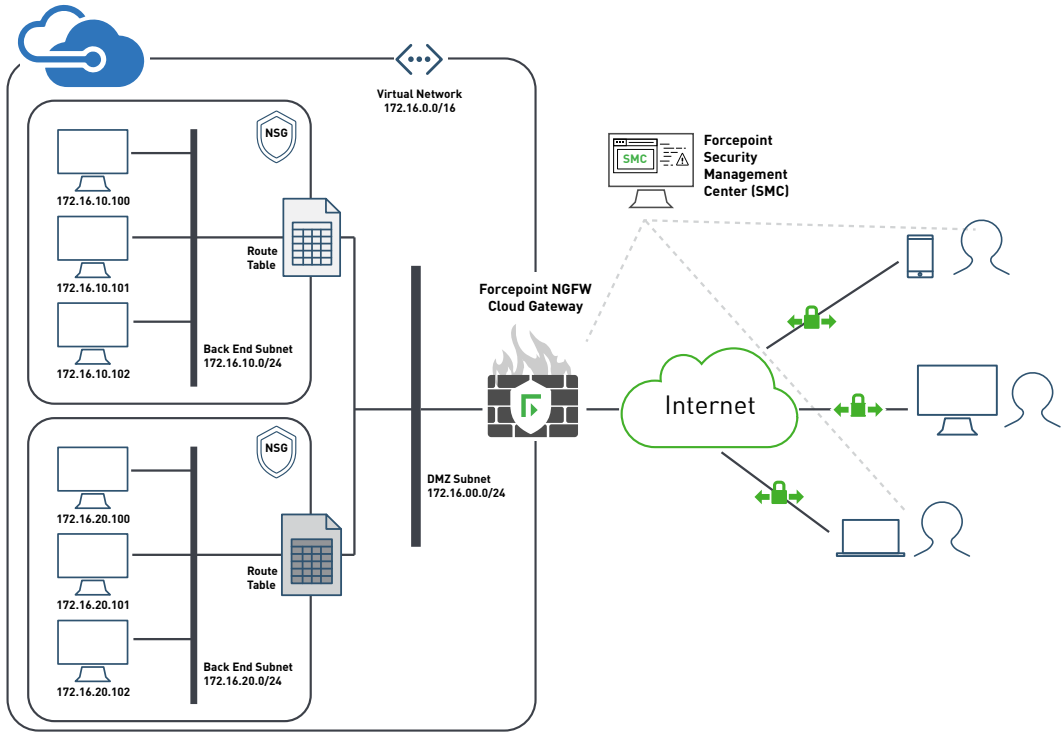
Remote access

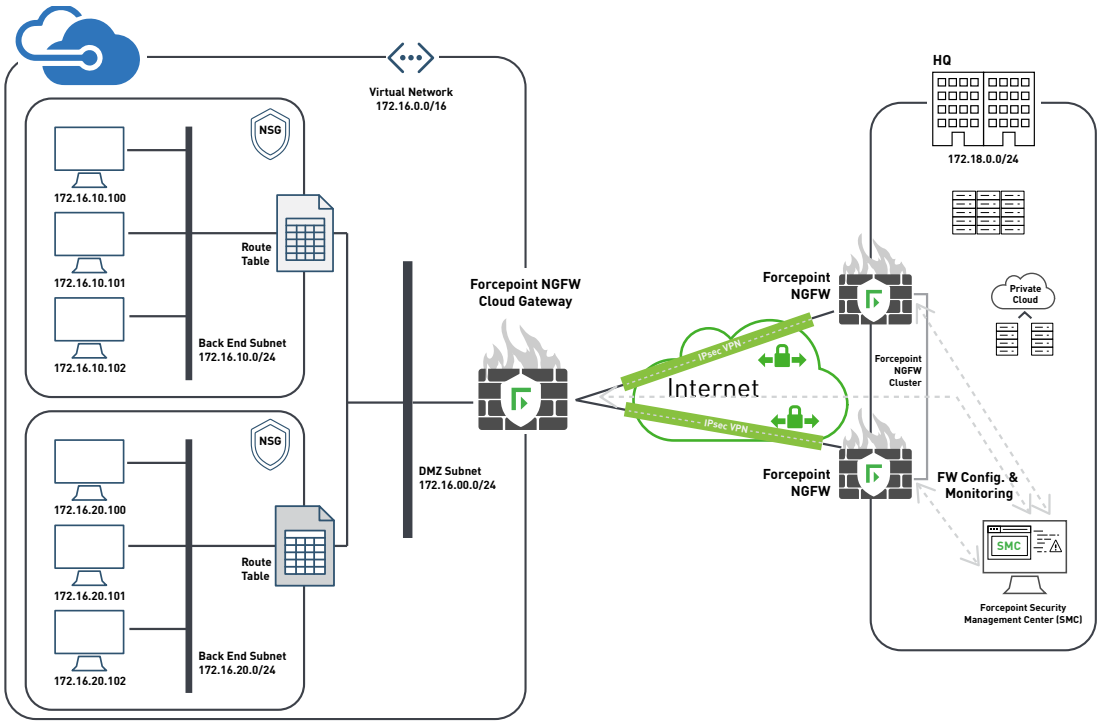
Quick and elastic deployment

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

Corporate data center connectivity

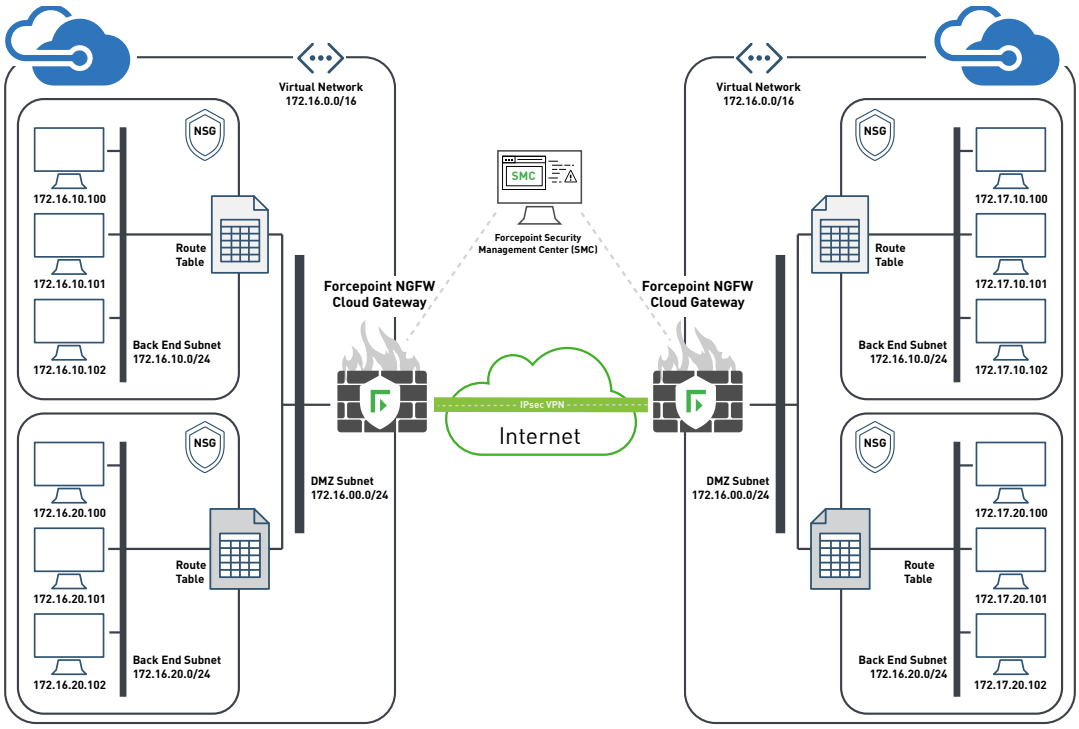
Forcepoint NGFW physical and virtual gateways securely connect your corporate on-premises data centers to your virtual ones in Azure cloud. Simply create one or more VPN connection between your data center network and your Forcepoint software VPN appliance running in your Azure virtual network. Manage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





Inter-regional vnet-to-vnet routing

Create secure VPN tunnels between two or more Forcepoint software VPN appliances to connect virtual networks within or across multiple Azure cloud regions. You can manage, control and enforce security policies at both ends of the VPN connection using Forcepoint SMC.



CONTACT
www.forcepoint.com/contact

© 2017 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

[SOLUTION_BRIEF_FP_NGFW_MS_AZURE_ENUS] 700008.101017