Forcepoint

Solution Brief

Forcepoint Next-Generation Firewall with Microsoft Azure

The most secure and efficient enterprise firewall–centrally managed, always on & relentless

Challenge

- Businesses and organizations need to maintain the same level of security over their cloud and hybrid environments as they did with traditional on-premises infrastructures
- Building and maintaining a secure cloud or hybrid infrastructure can be expensive and pose a technical challenge
- Regulatory compliance can be difficult to navigate and pose a technical challenge

Solution

- Forcepoint Next-Generation Firewall provides a software-centric solution that is uniquely designed to deliver maximum security with minimum cost and complexity
- Forcepoint Security Management Center (SMC) enables teams to manage thousands of firewalls, streamline processes, and provides unrivaled visibility with granular controls
- Our solution streamlines compliance effort by offering out-of-the-box policies to help ensure compliance across virtual and physical networks, as well as providing easy access to audit reports

Outcome

- Maximum cloud and hybrid security with minimum complexity
- Expedited incident response
- Streamlined regulatory compliance, implementation and management
- Lower Total Cost of Ownership (TCO) for network infrastructure and security

Forcepoint Next-Generation Firewall connects and protects demanding, distributed enterprise networks. Zero-touch elastic deployments and a Zero-Trust approach to network security provides the efficiency, reliability, and high security efficacy you need to defend your edge.

Trusted by thousands of customers around the world and available through the Microsoft Azure marketplace, Forcepoint network security solutions enable enterprises to address critical issues efficiently and economically, effectively helping them to get left of the breach.

Forcepoint Security for Public Cloud Environments

Cloud-based services and virtual deployments are transforming businesses of all shapes and sizes. Traditional on-premises hardware is rapidly disappearing because organizations need greater efficiency, agility, and cost control without the burden of maintenance and overhead. In order to help our customers stay competitive, Forcepoint has strategically designed our network security solutions to be software-centric, which means you can take them with you when you move to the cloud. The widespread adoption 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 software-centric solutions are uniquely designed to deliver maximum security with minimum cost and complexity. Our Security Management Center (SMC) provides a unified platform that offers unrivaled visibility, control, and consistent policy enforcement to help ensure regulatory compliance in physical, virtual, and cloud environments.

Microsoft Azure Cloud Security

To secure cloud environments, Forcepoint brings leading next-generation firewall technology to Azure 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 Azure cloud environment through 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. You can quickly zero in on what's happening in both your Azure environment and your physical network.

+ Customers who switch to Forcepoint Next-Generation Firewall report an 86% drop in cyberattacks, a 53% less time burden on IT, and a 70% decrease in planned maintenance.

Maximum Security, Minimum Complexity

The software-centric architecture of Forcepoint security solutions such as advanced threat protection, deep packet inspection, and application-level control is designed for easy, elastic deployment on-premises, virtually, or in the cloud. Granular user, application, and protocol controls enable your security team to leverage the power of automation to cut down on complexity and minimize time spent on mundane security hygiene tasks. The Forcepoint comprehensive and integrated defense-in-depth approach can be tailored to the specific needs of each person, place, or asset, including single or multiple firewalls, VPN, IPS, and URL filtering protection. Our comprehensive next generation firewall provides all of the existing capabilities of an advanced hardware appliance, including stateful inspection, granular policy and access control, and redundant ISP connections—but without the box.

Real-Time Visibility and Control

Forcepoint Next-Generation Firewall delivers complete visibility and control over the traffic flow within virtual and cloud environments that traditional management consoles cannot. Our renowned SMC provides rapid reporting as well as automated failover capabilities to alert administrators if a system is about to go down and make automated decisions based on pre-configured rules to help prevent any user experience interruption. 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 with a holistic monitoring dashboard that provides full-stack application visibility and granular controls.

Simplify 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 digital space is even more challenging. Traditional controls around each application are not present in a virtual environment, which makes determining which information was accessed by whom and when near impossible and is likely to raise a red flag to auditors. The Forcepoint SMC provides the level of monitoring, analysis and reporting you need to help ensure compliance across physical and virtual networks. It gathers comprehensive data on all network events and presents them in clear, easy-to-understand 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.

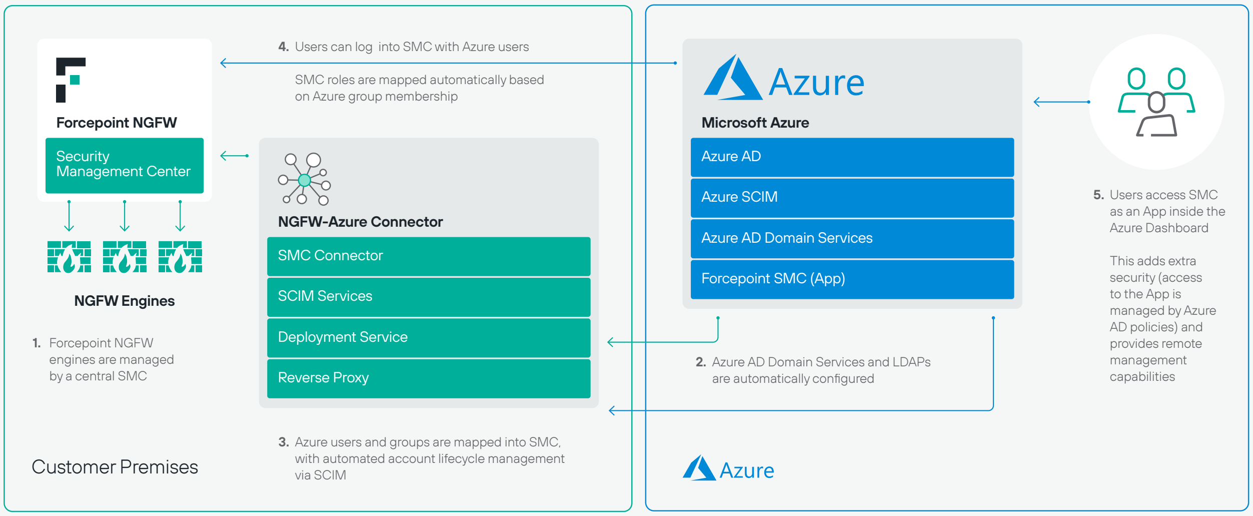
Quick & Elastic Deployment

To easily deploy Forcepoint Next-Generation Firewall in your Microsoft Azure environment, visit the Microsoft Azure Marketplce.

→ Visit Marketplace

Forcepoint Next-Generation Firewall + Microsoft Azure Solutions

Maximize your Azure investment and extend the capabilities of your Forcepoint solutions with our unique integrations. For more details on our integrations, including step-by-step implementation instructions, please visit forcepoint.github.io


Forcepoint NGFW
Security Management Center
NGFW Engines
1. Forcepoint NGFW engines are managed by a central SMC
Customer Premises
4. Users can log into SMC with Azure users
SMC roles are mapped automatically based on Azure group membership
NGFW-Azure Connector
SMC Connector
SCIM Services
Deployment Service
Reverse Proxy
3. Azure users and groups are mapped into SMC, with automated account lifecycle management via SCIM
Azure
Microsoft Azure
Azure AD
Azure SCIM
Azure AD Domain Services
Forcepoint SMC (App)
2. Azure AD Domain Services and LDAPs are automatically configured
5. Users access SMC as an App inside the Azure Dashboard
This adds extra security (access to the App is managed by Azure AD policies) and provides remote management capabilities
Azure

Azure Active Directory (AD) - Secure Hybrid Access Integration

Enables Forcepoint SMC access and authentication through Azure AD users and policies.

→ Exposes the SMC as an Azure app for remote management capabilities

→ Selected Azure AD users can be assigned different levels of access in the SMC, which allows for multiple remote management scenarios across an entire fleet of Next-Generation Firewall engines

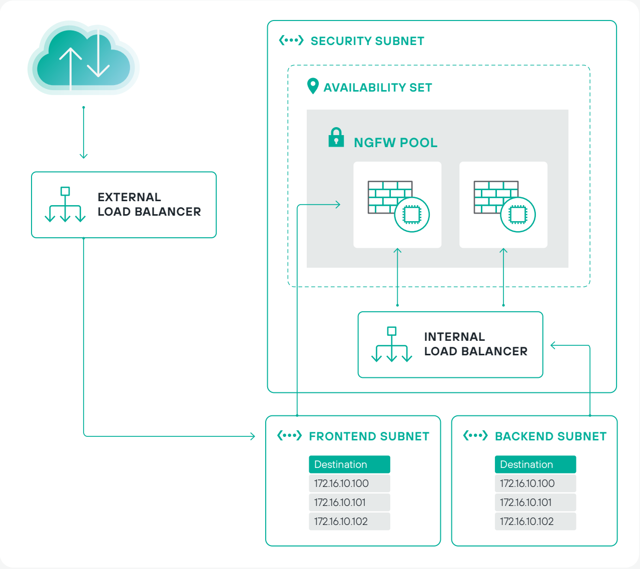
→ Enables centralized management and control within the SMC, but with the added security of Azure AD authentication policies

High Availability with Azure Resource Manager (ARM) Integration

Automates the deployment of a redundant set of Next-Generation Firewall engines in Azure, leveraging an ARM template configured to deploy the entire stack.

→ ARM template configured to deploy a stack that contains 2 network load balancers and 3 subnets to manage traffic between internal and external networks

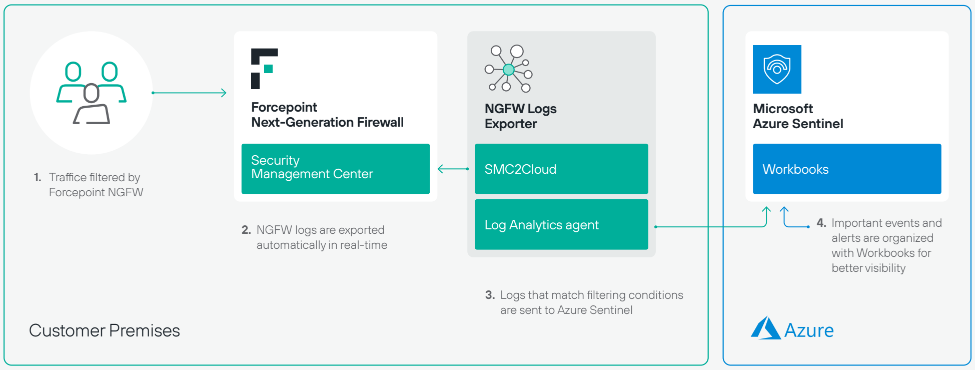
→ Enables Next-Generation Firewall engines to operate in high availability mode to provide uninterrupted network flow between users and workloads



Azure Sentinel Integration

Enables the exportation of pertinent log data from the Next-Generation Firewall according to user-configured filters.

→ Automatically export log events from Next-Generation Firewall into Azure Sentinel in real-time
→ Ingest logs into Azure Sentinel log analytics and visualize events using Workbooks

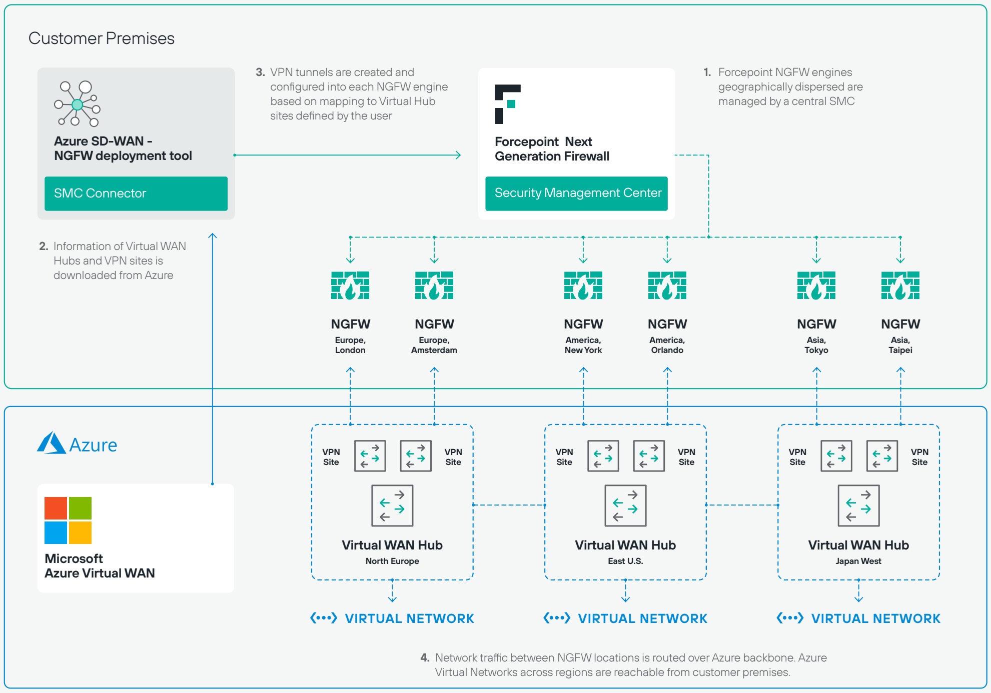


1. Traffice filtered by Forcepoint NGFW
2. NGFW logs are exported automatically in real-time
3. Logs that match filtering conditions are sent to Azure Sentinel
4. Important events and alerts are organized with Workbooks for better visibility

Azure Virtual WAN Integration

Enables automatic creation and configuration of IPsec tunnels between a fleet of Next-Generation Firewall engines controlled by Forcepoint SMC and geographical Virtual WAN sites.

→ Creates an SD-WAN layer that can be used to route traffic between sites over the Azure Virtual WAN backbone
→ Enables administrators to create redundant VPN tunnels in each Next-Generation Firewall engine controlled by the SMC using the IPsec standard
→ Allows for connection of VPN tunnels in each Next-Generation Firewall engine to specified Azure Virtual WAN regions



1. Forcepoint NGFW engines geographically dispersed are managed by a central SMC
2. Information of Virtual WAN Hubs and VPN sites is downloaded from Azure
3. VPN tunnels are created and configured into each NGFW engine based on mapping to Virtual Hub sites defined by the user
4. Network traffic between NGFW locations is routed over Azure backbone. Azure Virtual Networks across regions are reachable from customer premises.

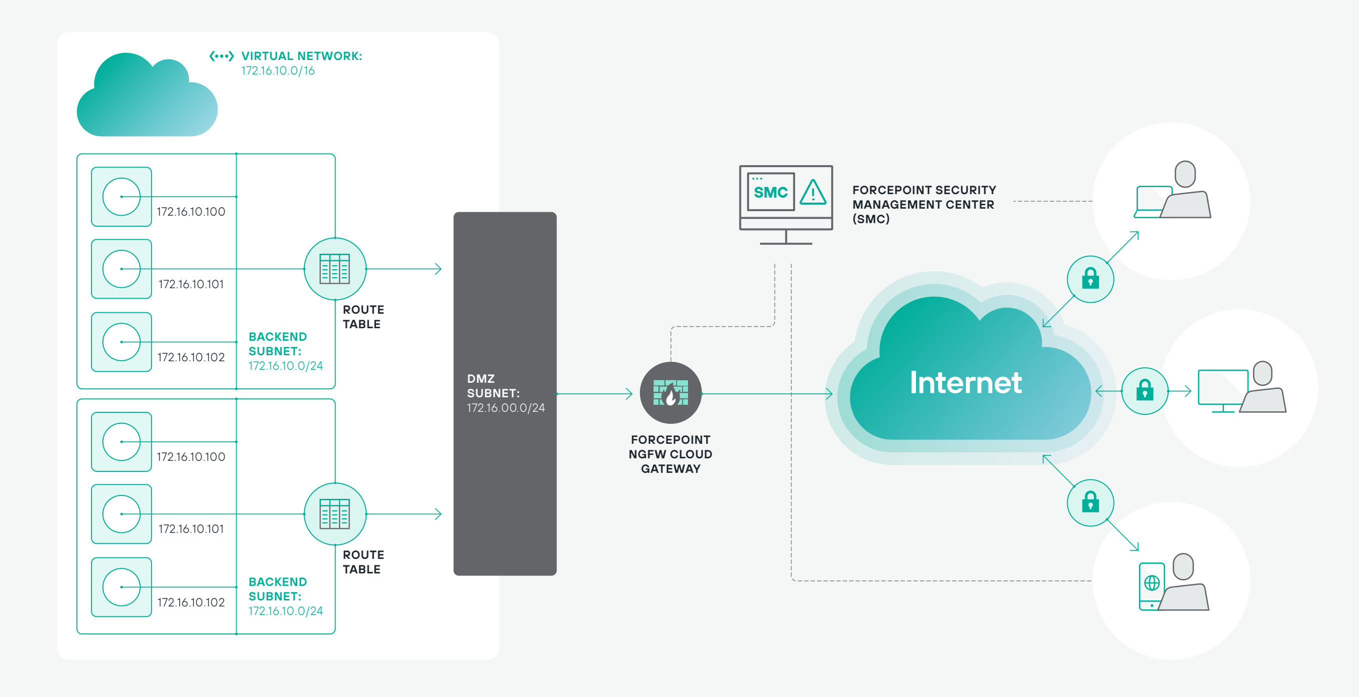
Corporate Data Center Connectivity

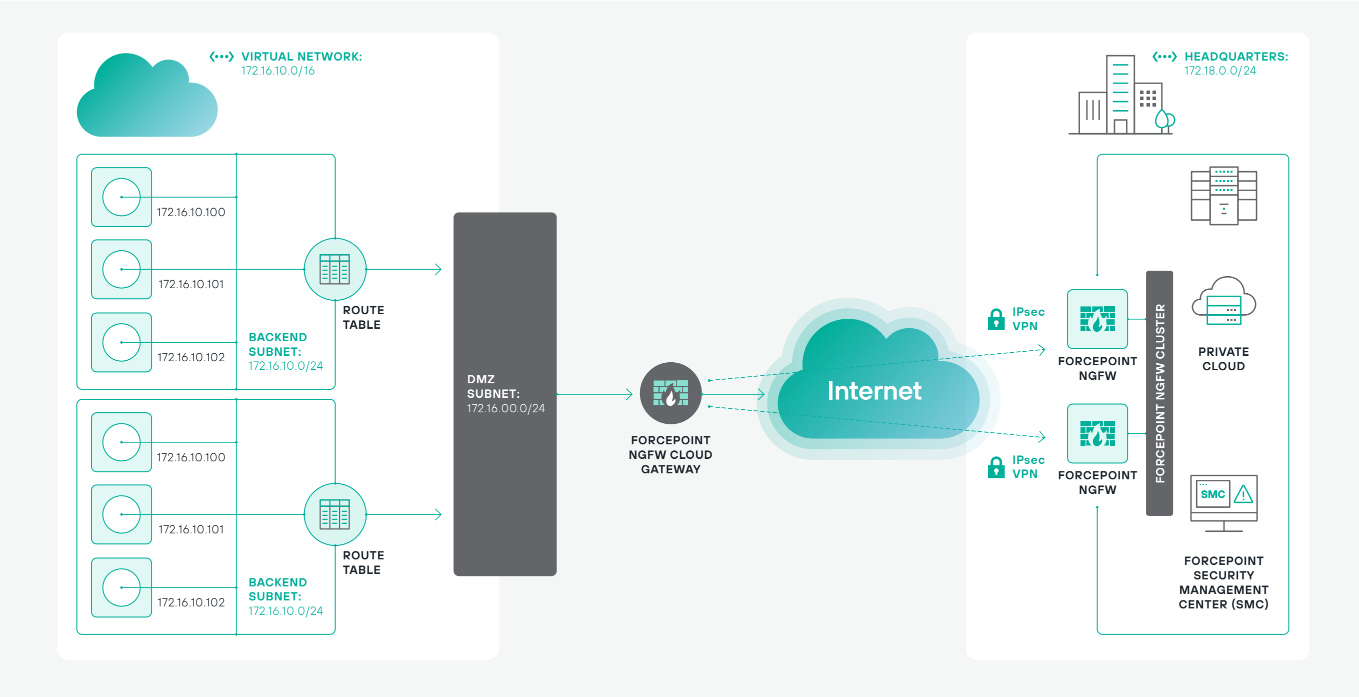
Forcepoint Next-Generation Firewall physical and virtual gateways securely connect your corporate on-premises data centers to your virtual ones in Azure cloud. For this use case, you can:

→ Simply create one or more VPN connections between your data center network and your Forcepoint software VPN appliance running in your Azure virtual network

→ Manage and control all your Forcepoint firewalls, both software-based and physical, at both ends of the VPN connections via the SMC

→ For business continuity on the headquarters side of the VPN connection, you can also use a cluster of physical firewalls for the purpose of failover.

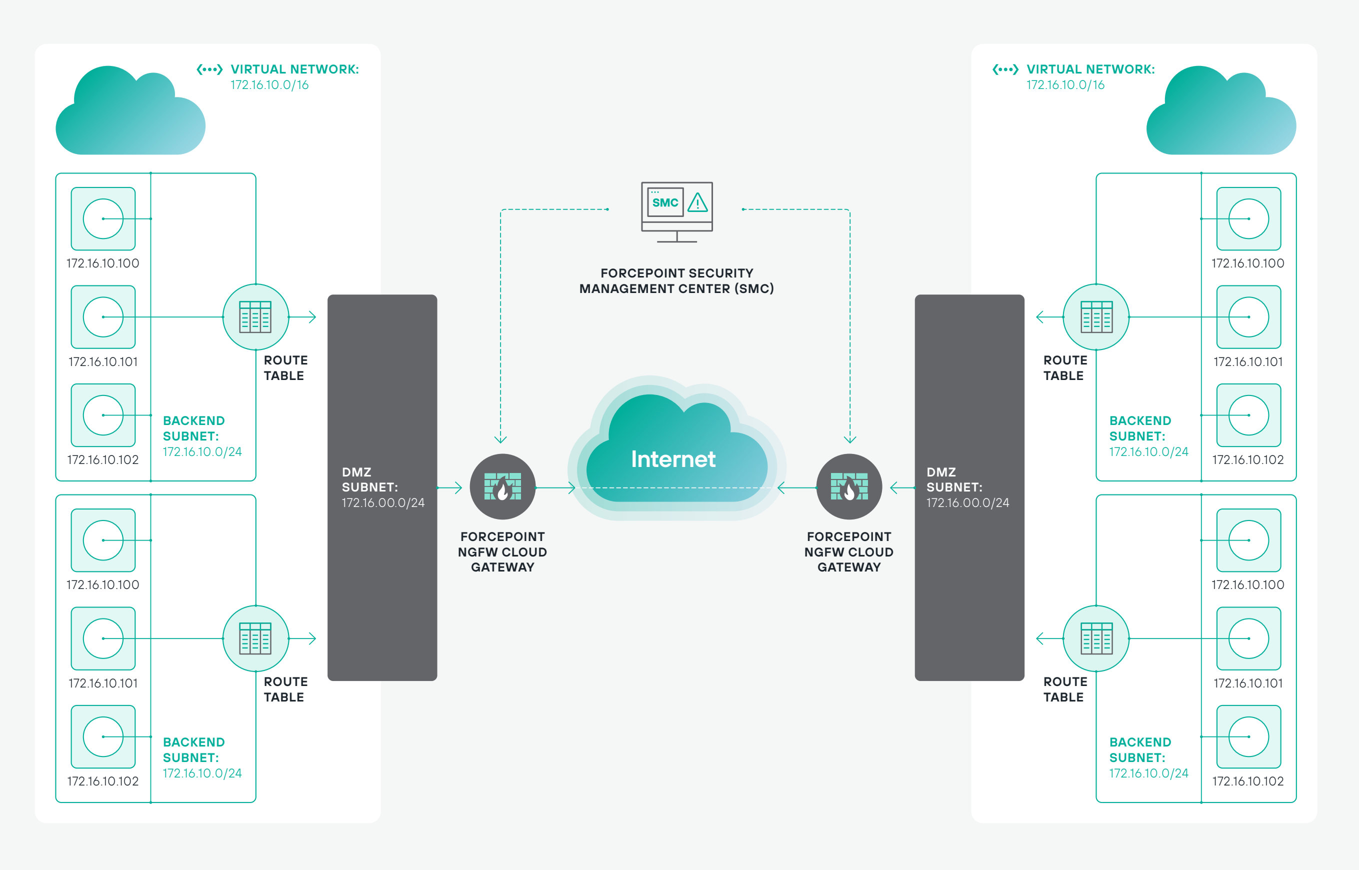




Inter-regional VNET-to-VNET routing

Create secure VPN tunnels between two or more Forcepoint software VPN appliances to connect virtual networks within or across multiple Azure cloud regions. For this use case, you can:

→ Manage, control, and enforce security policies at both ends of the VPN connection using the Forcepoint SMC


VIRTUAL NETWORK:
172.16.10.0/16
172.16.10.100
172.16.10.101
172.16.10.102
ROUTE TABLE
BACKEND SUBNET:
172.16.10.0/24
DMZ SUBNET:
172.16.00.0/24
SMC
FORCEPOINT SECURITY MANAGEMENT CENTER (SMC)
Internet
FORCEPOINT NGFW CLOUD GATEWAY
FORCEPOINT NGFW CLOUD GATEWAY
DMZ SUBNET:
172.16.00.0/24
VIRTUAL NETWORK:
172.16.10.0/16
ROUTE TABLE
BACKEND SUBNET:
172.16.10.0/24