SOLUTION BRIEF

Fortinet Logical (Intent-based) Segmentation for Cloud Environments

Executive Summary

Previously, network segmentation was relatively easy, with each entity using a static IP address and ingress/egress ports that were easily defined. But in distributed, multi-cloud environments, IP addresses—and the notion of trust itself—are constantly changing. As a result, network segmentation must change to remain effective. Intent-based segmentation from Fortinet enables organizations to partition their network according to business need, granting access according to role and current trust status. Every network request is inspected according to the requestor's current trust status, helping to prevent lateral movement of threats within the network.

Traditional Trust Models No Longer Work

Network segmentation has been around since the advent of the internet and was an important part of legacy perimeter-based security strategies. It enabled IT teams to provide employees (the primary users of the corporate network in those days) with access to only the resources they needed to do their jobs. It also inhibited intruders who did gain access from moving laterally within the network.

Accomplishing this was relatively straightforward when corporate resources were mostly in the data center, IP addresses were static, and ingress/egress ports were straightforward. But corporate networks now use highly elastic hybrid cloud configurations with dynamic provisioning, which results in constantly changing IP addresses. As a result, the trustworthiness of users, devices, and applications is in constant flux. This renders traditional "yes/no" trust models obsolete.

Logical (Intent-based) Segmentation from Fortinet

- Dynamically adjust security policies based on logical roles
- Automatically and dynamically create and/or terminate new cloud resources
- Inspect all north-south and east-west traffic
- Enforce consistent policies in a dynamic infrastructure

In a multi-cloud architecture, IP addresses are in constant flux, rendering traditional network segmentation useless.

Many recent data breaches, including the infamous attack on the U.S. Office of Personnel Management (OPM),[1] can be traced to the undetected lateral movement of adversaries within the network. The fact that such breaches continue to happen suggests that many companies are having trouble getting segmentation right.

Effective Protection Against Lateral Movement with Fortinet

Intent-based segmentation involves segmenting IT assets in line with business logic and user identity, and adjusting rules in response to continuous trust assessment. All traffic is examined, including north-south and east-west traffic.

The Fortinet intent-based segmentation solution for cloud environments is accomplished using Fortigate-VM next-generation firewall (NGFW) Fabric Connectors. This virtual NGFW leverages metadata and tags associated with cloud-based resources across multiple clouds as an element in defining dynamic address objects and in enforcing security policies. It intuitively defines which workloads and elements in the cloud are allowed to communicate with other workloads and elements—inside or outside that cloud. And Fortinet Fabric Connectors automate the process of keeping security policies integrated and consistent across multiple clouds. Creation and/or termination of new cloud resources do not warrant manual intervention by network and security administrators, as these changes are dynamically and automatically reflected in the dynamic address objects.

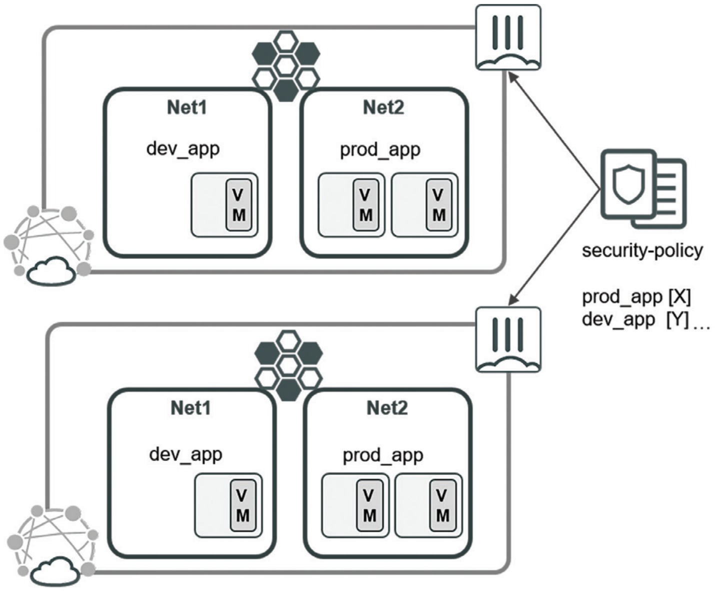

Figure 1. Intent-based segmentation: consistent rules based on business logic.

Fortinet intent-based segmentation helps organizations answer three basic questions:

- **Where the segments are demarcated**, according to business need
- **How trust is established**, with models kept up to date using continuous, adaptive trust
- **What enforces access control** across the entire network

Leveraging a Constantly Updated Trust Model

The increasing sophistication and speed at which threats propagate mean that effective segmentation is more important than ever. However, the constant evolution of an entity's trustworthiness means that they must be continually evaluated. Fortinet's intent-based segmentation solution ensures that every network request is inspected and verified based on current data.

[1] Josh Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," CSO, November 6, 2018.

www.fortinet.com