

Secure Dynamic VPNs

Juniper Networks has tightly integrated the benefits of a route-based VPN with the simplicity of rule-based firewalls to achieve a secure, resilient solution that is extremely easy to manage. The two main components that make the solution simple to deploy, configure and manage on an ongoing basis are:

Dynamic VPNs

With the Juniper Networks dynamic VPNs, enterprises can minimize the amount of time needed to spend managing their security and start concentrating on the things that are core to the business. With a Juniper Networks VPN device, enterprises can create logical VPN tunnels between destinations and then use dynamic routing to communicate network topology and link state information. As a result, enterprises don't have to worry about revising policies every time there is a change in the network and can feel confident that the VPN connection will be able to survive a failure.

Dynamic vs Static

Network administrators don't have the time to try and figure out the IP address for each and every machine that is participating in the VPN. But this is what most vendors force you to do. Instead of separating the logical and physical layers, these solutions tie them together in a policy that defines the VPN. What this means is that administrators need to define their network and then define the policy to explicitly state who can speak to whom through the VPN. This implies the use of a static route, which is very inflexible and gets increasingly difficult to manage for large or complex networks.

For example, with these legacy rule-based devices, every time a change to the network occurs, an administrator needs to make sure the change is made in the policy. If a VPN is added, the administrator has to list all of the IP addresses that it is responsible for and then make sure it is incorporated correctly in the policy. The list goes on and on. These changes grow exponentially as the network grows, forcing administrators to spend more and more time worrying about whether the VPN is configured correctly. Plus, if anything happens and a connection goes down, the administrator has to manually determine what's wrong and then manually reconfigure the policy. Because these solutions rely on human resources to keep the VPN up and running, they are prone to errors, which can ultimately lead to security compromises.

Dynamic, Intelligent VPN

With the Juniper Networks dynamic VPNs, enterprises don't have to worry about changes to the network and how they affect the VPN, saving time and resources. Juniper's dynamic VPNs automatically learn the network topology, so administrators don't have to define it, which reduces the likelihood of mistakes due to human error. If a connection goes down, the Juniper solution can automatically look for an alternate route to ensure the communication gets where it needs to go. Juniper Networks also adds a lot of other capabilities to further improve the resiliency of the solution to ensure that it provides enterprises with the "always on" connectivity they need.

Dynamic, Secure VPNs

The Juniper Networks IPSec VPN devices are tightly integrated with the firewall solutions, so enterprises can achieve the security they need, without introducing compromises or complexity. All other VPN and firewall solutions require either a sacrifice of security for simplicity, or changes throughout the IP addresses of the network when defining either the VPN or firewall, which eliminates the efficiencies of route-based management. For instance, some vendors that offer route-based VPNs add only rudimentary firewall capabilities, which leave the network vulnerable to potential unauthorized use (i.e. simple access lists applicable to packets to perform access control functions, inability to track the state of the communication or perform Stateful Inspection of protocols, easily circumvented authentication mechanisms). The other option that these route-based VPN vendors can offer to achieve robust firewall capabilities is to integrate their firewalls that require the specification of the IP addresses in the policy to differentiate between VPN and other traffic. As a result, this solution is no better than a rule-based VPN and firewall, in terms of the amount of management time that will be needed to keep the connections current and available.

Plus, these VPN and firewall solutions, whether they are delivered as separate devices or as separate solutions on the same platform, cannot be managed from a single interface. As a result, these solutions require enterprises to use different management interfaces, which increase deployment, integration and ongoing maintenance time.

Security Zones

The Juniper Networks integrated firewall/VPN solutions solve these problems, by providing robust firewall capabilities that can be managed in a way that leverages both the efficiencies of route-based VPNs and policy-based firewalls. This is achieved by using a security zone-based approach. This model enables the integrated firewall/VPN devices to separate the network into areas or zones that are protected from each other. The zones can encompass one or more physical or logical interfaces, including VPN tunnel interfaces. This means that IP addresses are not required by the firewall to differentiate the traffic, so there is no loss in the efficiencies of dynamic route-based VPNs. Instead the firewall uses the interfaces that are defined in each zone to determine what to do with the traffic, which actually simplifies not only the initial configuration, but also the ongoing management.

Basically, a security policy is created for each zone, and the firewall applies the policies between pairs of security zones to control the type of traffic that is permitted or not permitted to pass between the zones. When a new interface is added to a security zone, the policies that are in effect for that zone are automatically enforced on the new interface. This makes the integration of new sites into the VPN easy and quick, since all the organization needs to do is add the interface for the new site to an existing security zone.

The security policies that control what type of traffic goes in or out of a zone from traffic forwarding specifications are also decoupled. This allows a security policy to be dynamically associated with a VPN configuration. For example, a security policy can be defined that allows all traffic from the "HQ" zone to the "Remote Sites" zone. The routing table in the solution is able to determine which of several candidate tunnel interfaces is to be used to reach a given remote site. The tunnel interface status is reflected in the routing table, which permits automatic VPN link selection, while maintaining consistent policy enforcement. In this way, enterprises benefit from the simplicity of both a route-based VPN and a policy-based firewall and the integrated security for data privacy, access control and authentication.