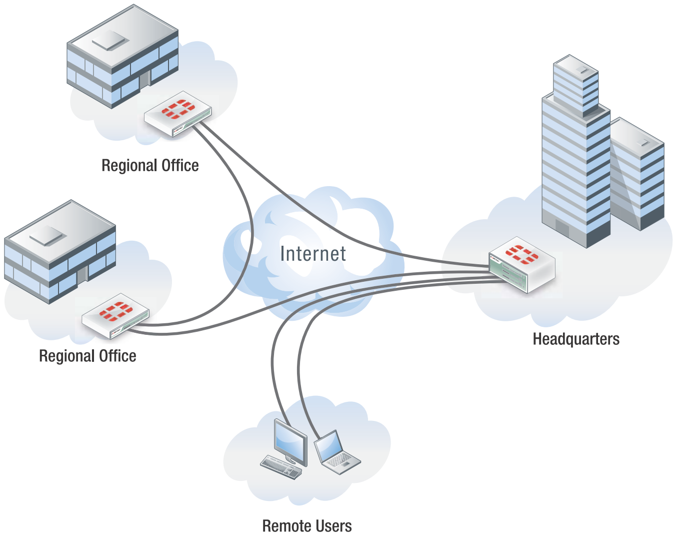
FORTINET®

SOLUTION GUIDE

Virtual Private Networks

Secured Connectivity for the Distributed Organization

Introduction



VPN Tunnels Using the Internet as Primary Transport Medium

A Virtual Private Network (VPN) allows organizations to securely connect multiple physical locations and users together using an untrusted public network, such as the Internet, as the primary transport medium. Moreover, mobile broadband, cable, and DSL providers have made notable increases in market penetration over the past decade, making access to high-bandwidth Internet connectivity almost ubiquitous. The increased adoption has also made these types of Internet connectivity less costly than private leased line alternatives. By combining VPN technology with common Internet access, organizations are able to extend the speed and reach of their network while also reducing costs.

VPNs provide high levels of security by encrypting data in transit to prevent unauthorized access. VPNs are generally divided into one of two high-level categories: *site-to-site* (also known as gateway-to-gateway) or *remote access* (also known as client-to-gateway or dialup). While the fundamental concept of providing an encrypted tunnel between two networked nodes remains constant in both categories, the implementation and technologies used to deliver the solution differ substantially.

Fortinet VPN solutions offer customers a broad range of options for establishing VPNs in both major categories by supporting IPsec, SSL-TLS, and L2TP VPN technologies. The Fortinet VPN solution is comprised of FortiGate® multi-threat security devices, FortiClient™ endpoint agents, and FortiManager™ centralized management. The Fortinet solution for secured connectivity integrates technologies not commonly found together into a single platform, which improves security, simplifies the IT environment, lowers total cost of ownership, and provides the most flexibility and choice when it comes to deployment options.

Site-to-Site VPNs

Site-to-Site VPNs commonly connect remote office and branch office locations back to a headquarters location. Some organizations also use site-to-site VPNs to establish limited access for trusted business partners to their private network. In both situations, a FortiGate multi-threat security device, or other supported VPN device, is deployed at each network location where VPN tunnels are to be established. FortiGate devices are then configured to establish an authenticated and encrypted tunnel, routing traffic through this virtualized tunnel between the sites and according to the defined policy.

There are varying VPN topologies for site-to-site tunnels, including *hub-and-spoke*, *partially-meshed*, and *fully-meshed* configurations.

- In a hub-and-spoke configuration, VPN connections radiate from a central FortiGate device (the hub) to a number of remote FortiGate devices (the spokes).
- With partially-meshed configurations, locations that commonly communicate with one another are configured to have dedicated VPN tunnels.
- Fully-meshed configurations connect all VPN peers to one another for the most fault-tolerance of the three deployment topologies.

IPsec is the most common technology used in customer-provisioned site-to-site VPNs. Provider-provisioned VPNs, defined as connections provided by a network or service provider, often use other protocols but are beyond the scope of this paper. IPsec is not a single protocol, but rather a suite of protocols. The various protocols within the IPsec suite are used to provide *integrity*, *authentication*, and *confidentiality* of data between VPN endpoints.

FortiGate devices support all commonly used VPN topologies. FortiManager centralized management platforms can greatly simplify the overhead associated with configuring highly redundant fully-meshed networks.

Remote Access VPNs

Remote access VPNs, also called client-to-gateway or dialup VPNs, connect a single host with the security gateway. The security gateway may connect tens, hundreds, or even thousands of unique remote clients to the private network. Many remote access VPN gateways use a single remote access technology, however products like the FortiGate system consolidate multiple access technologies into a common platform for simplicity, cost effectiveness, and maximum flexibility.

Most remote access VPNs use the IPsec protocol suite discussed in the site-to-site VPN section or the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. There are advantages and disadvantages to each technology and the best solution for remote access is often a combination of the two, allowing the best-suited technology to be used as needed.

IPsec-based VPN gateways, first discussed in the site-to-site VPN category, are capable of providing a remote user with the same access privileges as a local user. The disadvantage of this type of remote access VPN is that it requires a client on the remote user's system. Client-based systems lead to added complexity, but may be the best option in some situations to provide the most robust remote user experience.

SSL-TLS VPN (SSL-VPN) gateways are commonly viewed as a more flexible alternative to IPsec VPN gateways. The primary reason for their added flexibility is due to their use of SSL-TLS protocols, which are commonly found in modern Internet browsers. By leveraging a browser's cryptographic facilities, SSL-VPNs eliminate the requirement for a separate endpoint client. This clientless access method is usually more limited, however, than client-based solutions and remote access is typically limited to web-based applications. To address this shortcoming, many SSL-VPN gateways commonly also include a lightweight client that is dynamically downloaded, installed, and executed upon initial connection to the gateway. This lightweight client provides a more robust experience over the clientless option.

FortiGate systems include support for both major remote access VPN types in a single device, allowing them to support multiple remote access clients using multiple remote access technologies simultaneously on a single appliance. The systems also incorporate other critical security services that secure traffic entering the private network including: Firewall, Antivirus, and Intrusion Prevention. Providing gateway services and security inspection services in a single platform ensures that the remote access vector is secured and threats are not allowed to pass onto the private network, whether traffic is originating at a branch location or a single remote user.

Fortinet VPN Solutions

Fortinet VPN solutions allow distributed organizations of all sizes to be connected and secured. The Fortinet product family offers a fully integrated and complete end-to-end solution for connecting networks and users together, while also detecting and eliminating a wide spectrum of threats and malicious activity.

Fortinet meets the connectivity needs of any-sized organization while offering unmatched functionality and price-performance.

- FortiGate security platforms provide secure and cost-effective connectivity between two or more networked sites.
- FortiClient endpoint agents allow remote users to connect to centralized network resources securely and efficiently.
- FortiManager centralized management platform unifies all VPN provisioning and tunnel monitoring of the secured connectivity solution.

FortiASIC™ acceleration, found exclusively in FortiGate platforms, is key to providing the performance necessary to support IPsec VPN and SSL-VPN services, along with the full suite of services provided by FortiOS, on a common hardware platform. FortiASIC processors are custom-designed silicon which work to reduce the load on the general purpose processor associated with complex cryptography and other processor-intensive security inspection techniques.

FortiGate platforms go beyond basic VPN connectivity to provide a wide range of security and networking functions that are critical to an organizations security and network performance goals. Key services of interest to the distributed organization when using a FortiGate platform:

- WAN Optimization / Web Caching: Distributed organizations often suffer from poor application performance at remote locations. The WAN optimization function available in many FortiGate models allows organizations to accelerate WAN-based traffic and improve performance to more closely match local area network performance. By inspecting traffic and enforcing security policy from the same device, only authorized traffic is allowed through the secured and accelerated tunnel, further enhancing performance.
- Data Loss Prevention: Regulatory compliance governing sensitive data applies to branch locations and remote users as well as headquarters locations. FortiGate data loss prevention works to ensure that sensitive data is used according to policy. By extending data loss prevention to the branch location, visibility is also enhanced.
- Vulnerability Management: In a multi-location network, often the weakest point of entry is the brand location. Now FortiGate systems can use the FortiGuard Vulnerability Management service to perform vulnerability assessments at the branch location, eliminating what has typically been a huge blind spot in a vulnerability management program.

Summary

VPN technology has become a staple of modern IT infrastructure. With almost universal access to the Internet from any physical location, VPNs are a fast, efficient, and cost-effective way to connect remote locations and users. While the types of VPNs in use today are varied, the IPsec suite of protocols are prevalently used with site-to-site and remote access VPNs. SSL and TLS protocols are primarily used with remote access VPNs. FortiGate VPN solutions support site-to-site and remote access VPNs concurrently. They also support IPsec and SSL-VPNs concurrently. FortiClient endpoint agents provide client-based access and FortiManager centralized management facilitates all VPN configuration and monitoring, from FortiGate systems to FortiClient endpoints, from a centralized location.

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2009 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise – from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel +65-6513-3730
Fax +65-6223-6784