

News You Can Use: Perimeter Security

When securing a company's network, it's best to start on the edges — the perimeter — where the system interfaces with the rest of the world. While installing safeguards deep inside the network is a good idea for securing against some types of threats, you'll generally get the broadest protection — and the biggest bang for your security buck — by building up protection along the edges. When planning a perimeter-oriented network-defense strategy, one has to understand exactly where the perimeter lies and what technologies are involved. Put simply, the perimeter is the network's boundary: the frontier where data flows in from (and out to) other networks, including the Internet. Perimeter defense functions like a checkpoint, allowing authorized data to enter unencumbered while blocking suspicious traffic.

This article will discuss Perimeter-checkpoint duty and how it is handled by different technologies, including border routers, firewalls and a variety of other specialized security products. Today, we begin looking at each of these technologies by learning about the first technology: Border routers.

Border routers: Network routers work much like traffic cops, directing data into, out of and within networks. A border router is a special type of router: the one that stands between your network and an external network, such as the Internet. Therefore, the border router is like a traffic cop posted at a spot located on the way into town — the one who spots the license plate on the bad guy's car. Since all Internet traffic passes through the border router, it's a logical place for filtering.

Firewalls: A firewall's basic job is to permit or stop data flowing into or out of a network. For perimeter defense, firewalls are available as software (installed inside a router) or as stand-alone hardware appliances. A firewall can provide services such as state inspection (analyzing transactions to ensure that inbound packets were requested); packet filtering (blocking data from specified IP addresses and ports); and NAT (network address translation), which presents a single IP address — representing multiple internal IP addresses — to the outside world.

IDSes (Intrusion Detection Systems): An IDS protects networks by analyzing traffic for suspicious activity. If something unusual is detected, the IDS alerts the network administrator, who can then take action to stop the event that is taking place. In fact, an IDS is often described as a network burglar alarm. Various vendors offer IDS products with a range of different capabilities, enabling customers to easily find a system that most closely matches their security and budget needs.

IPSeS (Intrusion Prevention Systems): An IPS is similar to an IDS, except that the product is designed to take immediate action — such as blocking a specific IP address or user — rather than simply issuing an alert. Some products also use behavioral analysis to spot and stop potentially dangerous data. The line between IDS and IPS technologies is blurring, so it's now possible to find an IDS that incorporates IPS functions.

VPNs (Virtual Private Networks): A VPN provides perimeter security by encrypting the data sent between a business network and remote users over the Internet. In essence, the technique creates a private tunnel through the Internet. VPN technology is widely popular and is used by enterprises of all sizes. The approach's biggest threat is from an attacker who figures out a way of compromising an authorized user's system, then gains control of an encrypted pathway into the company network.

DMZs (Demilitarized Zones): Borrowing its name from the no-man's-land created between North Korea and South Korea at the end of the Korean War, a DMZ is a neutral area that is created outside the firewall between a company's network and an external network, such as the Internet. One way of forming a DMZ is to install a host (a dedicated server) that resides between the two networks. The DMZ host can initiate sessions for Web pages, email and other requests on the public network. The system can't, however, initiate a session back into the company's network — it can only forward packets that have already been requested. The technique prevents unrequested and potentially destructive data from entering a company's network.

Perimeter network security works by providing several layers of protection at the network's edge. Different security technologies working in unison create a fortress-like barrier that can thwart sieges launched by most types of attackers and snoops. Perimeter security can't, however, block all attacks — particularly a DoS (denial-of-service) onslaught. Yet a well-planned system will efficiently deflect most network threats, providing peace of mind for business owners and managers, network administrators, and end users.