Firewall solutions for small and medium enterprises

Does the 'All-in-one' firewall device meet the requirements of small and medium-sized enterprises? For those who are responsible for managing computer networks for organizations and businesses in the environment. Today's business school is probably security - data security is the top issue in every situation.

Does the 'All-in-one' firewall device meet the requirements of small and medium-sized enterprises? For those who are responsible for managing computer networks for organizations and businesses in the environment. Today's business school is probably security - data security is the top issue in every situation.

Picture 1 of Firewall solutions for small and medium enterprises

Picture 2 of Firewall solutions for small and medium enterprises

One of the most effective and most commonly used tools is to use firewalls to control external access to the intranet and network transactions.However, investing in a firewall is quite expensive, especially for organizations - small and medium enterprises.In this case, perhaps a device solution that can handle all safety functions is most reasonable.This 'All-in-one' security device must meet the organization's and enterprise's security - data security requirements in the most efficient way without the need for many expensive and complex equipment layers, plus add a full-time staff.This is very necessary in the current situation that the Internet is full of threats such as worms, programs that destroy and steal information, security holes of operating systems and applications.

The article presents the latest firewall products of three suppliers in Vietnam: Check Point's Safe @ Office, Juniper Netscreen-5GT Enhanced and SonicWALL Pro 2040.

Experiments show that manufacturers have not only different definitions around security but they also have very different opinions about what it means to be 'Equipment'.

Check Point SAFE @ OFFICE 225

Belonging to the expensive security product line and running complex operating systems, Check Point's Safe @ Office except the name is hard to call and this is an excellent player on the small office 'ring stage'. and family (SOHO - Small Office / Home Office).

PARTY IN A VPN CONNECTION

VPN connection consists of 2 stages, each setting its own encryption and authentication protocol.Phase 1 set up an IKE (Internet Key Exchange) channel.Phase 2 is the IPSec channel, acting as armored vehicles running along the established ghost road in phase 1.Phase 2 sends data, protects data under 2 separate encryption layers.When phase 1 is completed, the heaviest part is considered to be completed, and adding the number of channels in phase 2 only increases the insignificant load for the firewall.

Picture 3 of Firewall solutions for small and medium enterprises

The fact that it is the easiest to configure in six products, even more impressive when you discover it runs Firewall 1, the most powerful and expensive platform of Check Point.Although running Firewall 1 inside, managing Safe @ Office is not complicated, thanks to a well-designed web interface.The 'Services' tag concentrates most of the features needed to administer Safe @ Office, including dynamic DNS, dynamic VPN and anti-virus in e-mail.These features are connected via the Internet to Check Point servers to automatically update and help set up.

Picture 4 of Firewall solutions for small and medium enterprises

Picture 5 of Firewall solutions for small and medium enterprises

Although this device is powerful enough to protect a large enterprise network system, it only belongs to the SOHO product line.Check Point limits 10 connections at the same time (test device);and 10 VPN connections, including both LAN-to-LAN connections and from client-to-LAN connections.With the SOHO scale, Safe @ Office makes network security management easy.

Check Point features are very stable connections.The standard VPN connection can be IPSec - free download from Check Point - or PPTP (Point to Point Tunneling Protocol), meaning it supports Microsoft VPN.In addition, the client can be authenticated against an internal database or a RADIUS server.This device also allows static routing, which means you can have multiple subnets behind the firewall as well as routing functions.

The testing process showed that Safe @ Office is indeed a very effective firewall.It prevents simulated attacks and repels all 'sneaky' ping commands from the WAN to the DMZ or LAN.

Safe @ Office has its own way of preventing viruses.This device sends emails to a Check Point server to scan for viruses, then transfer them to destination addresses.This explains why a small CPU can perform many services at once, but this also means that Safe @ Office cannot check for viruses that have been downloaded before installing this device.

Final conclusion?Check Point has 'pulled out' its famous Firewall product to build Safe @ Office.With a user-friendly interface and a focus on handling advanced features such as anti-virus, web filtering and DNS dynamics at Check Point servers, Safe @ Office has many complex features that cost less, in return. Users must depend on Check Point's services.

Picture 6 of Firewall solutions for small and medium enterprises

Juniper Netscreen - 5GT Enhanced

The tiny NetScreen-5GT Enhanced box has a good impression thanks to the integration of all the features that users require in a security device, including: firewall, VPN, intrusion detection and antivirus.Yet its price is very attractive, 495USD (US price) for 10 VPN connections.

Picture 7 of Firewall solutions for small and medium enterprises

Picture 8 of Firewall solutions for small and medium enterprises

The main interface of NetScreen-5GT Enhanced is designed to be very reasonable, you don't need to 'dig' anything inside if you just need to see the status of the firewall and the device is capable of responding in situations. emergency.Compared to similar devices, in addition to the basic functions, NetScreen also has the ability to prevent common attacks, including WinNuke, ICMP / UDP and SYN, Java / ActiveX destructive software and much more.

This device displays responsive to attacks in the form of menu, you can set it to just need to sound an alarm or start removing destructive packets, in this mode the device prevents Get all common attacks during testing.

The antivirus capability of this device is also very impressive.Similar to Check Point's Safe @ Office, NetScreen handles antivirus by registering services and Juniper's partner is TrendMicro.This device distinguishes the anti-virus settings for webmail and POP3 / SMTP e-mail services, but it does not support anti-virus for IMAP users.

Similar to the best rated device this time, NetScreen's VPN feature has passed the test very smoothly, it handles all 20 channels of VPN without any problems.

NetScreen is fully capable of protecting SOHO or small and medium enterprises, about 50 computers.This device not only supports connecting to multiple ISPs for redundancy, but also can dial the connection in case the WAN connection is interrupted.Another example is the Web content filtering feature that allows NetScreen to access WebSense's subscription service to create a list of banned or accessible websites (for a fee).

HOW TO TEST THE FIRST TEST OF TEST CENTER - INFOWORLD

Although manufacturers integrate different features in their 'All in One' firewall device, testing only focuses on three core areas: VPN performance, room capacity. Against attacks and viruses.
VPN performance evaluation: Which device performs the best data segmentation into packets, encrypted and sent over VPN channels. Testing Spirent Communications' TeraVPN version 4.0 toolkit installed on SmartBits 600 (SMB-600) installed 2 TeraMetrics XD communication cards, each card has a 10 / 100Mbps port.
• First, just run a VPN channel to make sure VPN works, then increase it to 20 channels. A small or medium sized business with 100-200 employees usually only needs up to 20 concurrent VPN connections. First, create 20 stage 1 channels (IKE), then in each channel create a stage 2 channel (IPSec). For the first time, to keep the packets fixed at 1024byte, the next time we change the capacity of the packets from 64byte to 1350 bytes, each step is done 50000 times.
• Evaluate basic firewall functions: Use Spirent's Avalanche / Reflector software on SMB-600 to create attacks. First, open up small DDoS attacks on each firewall to see if they detect and react, at least to sound an alarm. EdgeForce Plus, NetScreen and Safe @ Office work very well, they not only warn but also start eliminating attack packets. After that, continue to use stealth attack, how to ping the firewall. Conclusion: as long as the user is set up correctly, firewalls can prevent normal attacks.
• Anti-virus assessment: Set up a Linux server running Sendmail outside the firewall to send virus packets to a series of computers running behind the firewall.All viruses are simulated codes provided by the European Computer Virus Research Institute.All devices that pass this test are very smooth, but not all anti-virus for users using IMAP protocol.

The only feature not found on other devices is NetScreen's source routing capability.All tested devices allow for static routing, but only NetScreen can add 'source routing' declarations, so that users know where the route comes from and where the source comes from. OSPF (Open Shortest Path First), RIP (Routing Information Protocol), Boundary Gateway Protocol (BGP) or static routing.This is really the function of a high-end firewall integrated into an easy-to-use device.

Sonicwall PRO 2040

This medium-sized enterprise firewall can meet all requirements, it is easy to spot this when taking the device out of the box, it can be placed on a table, on a shelf, or installed in a 1U rack. All right.SonicWALL Pro 2040 combines SonicWALL's new generation SonicOS operating system and a good load-bearing hardware architecture, as long as you configure it correctly, of course, not simple.

PRODUCTS IN THE VIETNAMESE MARKET

Security is currently a 'hot' issue in our country, so if you are interested, you can find out the product information of the companies that are officially present in Vietnam through distributors.
Check Point: MISOFT (08-844 3027, 04-933 1613);Juniper: Juniper Networks Vietnam;SonicWALL: ITC JSC (04-943 0724, 08-925 3304).We tried to contact these distributors to ask for selling prices in Vietnam.However, until this article is printed, only Check Point product information: Safe @ Office 105: 614 USD, Safe @ Office 110: 1,071 USD, Safe @ Office 225: 1,887 USD, Safe @ Office 225U: USD 2,980.(information provided by MISOFT).Price does not include VAT, installation and deployment fees.Customers receive technical support during the process of using the product.

When used, users must install the SonicWALL extension OS to exploit many advanced features such as connecting to multiple ISPs for redundancy, load balancing with other Pro 2040s, setting NAT based policy and Redundant WAN connection.

Although Pro 2040 can be operated without the SonicOS Enhanced operating system, but you must install this OS to enable the device's fourth communication port.This port can function as a WAN, LAN, or DMZ port, or connect to another Pro 2040 device for backup.SonicWall is not inferior to rivals, it also integrates virus prevention and content filtering functions.

Pro 2040 is quite satisfying, for example, it is equipped with a processor that only makes each encryption task so the performance is no different when using AES-256 or 3DES encryption mode.A series of simulated attacks as well as preventing viruses when tested are prevented by this firewall.However, for the price of 1995 USD (price in the US), Pro 2040 should have more attractive features than NetScreen-5GT, the price is only 495 USD

Quoc Thanh
Infoworld