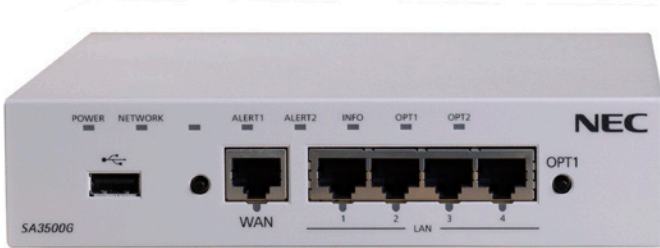\Orchestrating a brighter world

NEC

Unified Threat Management (SA3500G)

At a Glance

- Threat management appliance that provides an extra layer of security to a network to help combat against various cyber attacks

- Subscription-based anti-virus software scans for viruses in emails, when browsing the web or communicating with other applications

- Detects unauthorized access and unwanted intrusions

- Prevents access to malicious web sites

- URL filtering capabilities block access to harmful or non-business related sites or keywords

- Protects against the spread of viruses by limiting use of applications that freely exchange information

- Easy installation and configuration

- Provides up to 700 Mbps throughput even when security is enabled

- Works on any network

Overview

When you think about cyber-attacks, most likely, big corporations come to mind. They are usually the ones you hear about in the news reporting data breaches and ransomware attacks. In reality though, small and medium size businesses (SMBs) are actually being targeted more frequently.

As reported in the "2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB)" by the Ponemon Institute, in September 2017, 61 percent of the respondents said their companies have experienced a cyber-attack in the past 12 months, and 54 percent report they had data breaches involving customer and employee information in the past 12 months. In the aftermath of these incidents, these companies spent an average of $1,027,053 because of damage or theft of IT assets. In addition, disruption to normal operations cost an average of $1,207,965.

Cyber-attacks are a serious threat to your business and bottom line. With NEC's Unified Threat Management (UTM) solution, it adds an extra layer of security to your network to help combat these threats. UTM is a security device that helps protect your network and enhance your overall security from various cyber-attacks.

Solution

NEC's Unified Threat Management solution is a subscription-based service that offers the latest in threat management through an easily installed device that adds extra security to your network. As it sits between your router and your business's network, it combines multiple functions to prevent employees from accidently accessing dangerous sites, thwart unauthorized access from the Internet, and detects/cleanses viruses included in files attached to emails sent or received or downloaded from the web.

Threat Management Functions

Antivirus

Viruses, Trojan horses, Spyware, Ransomware and Worms are continually being produced and launched in efforts to disrupt, gather private and proprietary information, and hijack data for monetary gains. While businesses and employees need to be ever vigilant, you can implement extra security with the UTM that helps to eliminate the issue before it is allowed into your network. When a virus or dangerous code is detected in a downloaded file by the UTM, it cleans it by rewriting the contents of the file. Also, with the UTM's subscription-based model, your antivirus software is continually updated to help protect your network from the latest threats.

Intrusion Prevention System

Helps prevent unwanted network attacks by detecting patterns and matching intrusion methods previously registered. Once abnormal protocol, abnormal traffic or port scan is detected, it prevents further communication from the attacker with the network.

Web Guard

Most all employees have access to the Internet these days which means they are susceptible to phishing and dangerous websites that can potentially infect your network with a virus. With UTM's Web Guard, when traffic to a dangerous website is detected, access to the unsafe site is intercepted and denied.

URL Filter

With the Internet access afforded employees, companies may want to block access to certain known malicious sites and/or non-business related ones. UTM allows administrators to specify website categories to be blocked beforehand. When it identifies a URL from one of these categories, it denies access.

URL Keyword Filter

URL Keyword Filter acts in much the same way as the URL Filter. During web set up, specific character strings are registered beforehand and when someone types in a URL with one of these particular character strings, access is blocked.

Application Guard

Businesses may want to limit the use of some applications which can freely exchange information such as collaboration tools for file, software and video sharing as well as some messenger applications. Use of these apps could potentially open up a business's network to malicious viruses spread from the other party and information leakage. When someone tries to utilize one of these apps, Application Guard identifies, intercepts and prevents access. During web setup, the applications to be blocked can be entered. UTM regularly and automatically updates security signature definitions of viruses, malicious programs, and phishing sites for the period the product is licensed for.

Security Log and Email Notifications

All of the threat management functions mentioned above generate log messages when a threat is detected. The information captured is detection date, name of the detecting function, detection contents and the Internet Protocol address of the terminal to be detected. The Security Log's monthly statistics can be scheduled to be sent to the administrator and saved for future reference. When a threat is detected, not only is a log of it saved, but an email notification is sent out to appropriate personnel that one has occurred.

High-Speed Transmission

With all of the combined security functions of the UTM, you would probably assume it would affect network throughput. Typically, when adding security measures to a network, the speed of it tends to slow down. The UTM is built to enhance network security while not impeding the transmission rate of your network. Its 700 Mbps high-speed throughput is achieved by utilizing a high-speed security engine. Enhancing security no longer means a slower network.

Ease of Installation and Configuration

Installing the UTM in your network is as easy as connecting the WAN port to your router and the LAN port to your network. Once connected, the easy to use web set up allows you to customize threat detection according to your business's requirements.

Security Scan Function	Detection Type	Description
Antivirus	Threat Detection	Detection and removal of virus (data rewriting)
Intrusion Prevention System	Threat Detection	Prevention of network attacks
Web Guard	Web Access Control	Detection and interception of malicious websites
URL Filter	Web Access Control	Website category is identified and blocked
URL Keyword Filter	Web Access Control	Detection and blocking of a website that contains customer-defined keywords
Application Guard	Application Access Control	Identification and interception of applications that enable sharing of information on the network

Note: Encrypted packets are not supported by Antivirus, Intrusion Prevention System, Web Guard, URL Filter, URL Keyword Filter and Application Guard

---