Automatic Cyber Defense Enabled by Software Defined Networking
Software Defined Networking enabled Automatic Cyber Defense automates and enhances a network administration ability to protect against cyber attacks.

At a Glance

- Reduces the risk of information leaks, system shut-down, Denial of Service attacks, ransom-ware
- Enables faster response to cyber-attacks by automatically blocking infested workstations
- Enables the enterprise network micro-segmentation and installs virtual firewalls between segments, thus confining potential threats
- Allows quick identification of infested workstations
- Works in conjunction with leading firewalls and Intrusion Detection Systems such as SonicWall and Palo Alto
- Enhanced network management by using NEC ProgrammableFlow SDN controller

Overview

Increasingly sophisticated cyber-attacks are causing ever increasing damage worldwide. Survey data suggest that 80% of leaked information is obtained through external cyber-attacks. Viruses or malware can penetrate an enterprise network environment and steal information over a period of months, or even years, by cleverly concealing themselves. By the time the crime is uncovered, the important information has often already been leaked. Hacking methods are becoming increasingly devious and complex, making it extremely difficult for individual companies to mount an effective response alone.

Solution

Award Winning Software Defined Architecture

NEC’s ProgrammableFlow SDN is at the core of the Automatic Cyber Defense solution and it was the first commercially available Software-Defined Network solution to leverage the OpenFlow protocol. Network administrators leverage NEC’s SDN technology to achieve greater service agility through network automation and are able to control costs by consolidating network equipment. NEC’s ProgrammableFlow SDN solutions simplify network operation and increase network visibility, improving service levels by fine-grained control and visibility of network traffic.

A security appliance (e.g. Firewall or IDS) reduces risks of attacks and threats by providing perimeter protection, however does not ensure protection inside the perimeter. The organization is exposed to risks such as same-day attacks (that use vulnerabilities that are not yet detected by firewalls) or threats that originate inside the perimeter - attacks from workstations, from infested magnetic media brought from outside the perimeter.

ProgrammableFlow SDN allows the network to be virtually micro-segmented based on administrator defined criteria. Because of this unique network virtualization capability, network segments are independent from the physical layout of the network and can be modified as the network evolves. By combining the NEC ProgrammableFlow Controller with security appliances such as SonicWall and Palo Alto it is possible to enhance the protection inside the perimeter by identifying infected devices in one of two ways:

- An in-line security appliance identifies infected traffic from a device on the network
- TAP or SPAN traffic is sent to a security device for inspection

When the security device detects suspicious activity it instructs the ProgrammableFlow (using a dedicated software adapter) to isolate, redirect (to honeypot or other device), or drop traffic from the IP address of the workstation where it originated, thus preventing the damage from spreading. The network administrator is notified by E-mail of the action taken. This is achieved in seconds or tens of seconds (because of the automation) as opposed to minutes or days if done manually, without affecting other traffic in the network.
Implementing NEC's Automatic Cyber Defence SDN solution offers tremendous and significant Capital Expenditures (CAPEX) savings that are achieved via NEC’s ProgrammableFlow virtualization and abstraction capabilities.

Instead of segmenting the enterprise network at a physical layer, using an increased number of switches, copper and fiber cables and a complicate layout, it is possible to do it virtually, by using the ProgrammableFlow Virtual Tenant network (VTN) capabilities. The VTNs can be managed independently and subject to different access rules. They can be also separated by virtual firewalls that eliminate the need for multiple physical appliances.

With its resilient architecture, NEC’s solution also offers improved Operating Expenses. By virtualizing the network using NEC’s SDN, the network administrators no longer need to spend time and money to handle extremely complex infrastructure. Unlike traditional networks, the additions, movements or changes of endpoints in the network can be easily managed by the centralized controllers with minimal manual interventions.

SDN Standards-Based Eco-System

OpenFlow is a switch control protocol and the industry standard to achieve SDN. In conventional networks, each network device has route control functions and packet transfer functions. In an OpenFlow network, the route control function is decoupled from the packet transfer function enabling centralized control of networking. ProgrammableFlow is a network technology family, based on the OpenFlow protocol that enhances the basic functionalities of OpenFlow with technologies commercialized by NEC.

NEC’s Automatic Cyber Defense Solution Components

- Firewall (physical or virtual appliance) from SonicWall, Palo Alto or other supported supplier.
- NEC ProgrammableFlow used to control traffic in the enterprise Software Defined Network.
- NEC SDN Security Adaptor used to scan the logs generated by the firewall for possible threats and instruct the ProgrammableFlow controller to block traffic from workstations that show suspicious activity and notify the system administrator.
NEC’s Automatic Cyber Defense SDN Solution Synopsis

1. The firewall detects unauthorized communications; notify detected information to a SDN security adapter
2. The SDN Security Adapter generates appropriate security measures; instructs an SDN controller to take an action based on the result
3. The ProgrammableFlow Controller (PFC) takes an initial action by blocking selected communication flows
4. ProgrammableFlow Switches (PFS) block certain terminals communication as instructed by PFC