FORTINET | NEC

SOLUTION BRIEF

Fortinet and NEC SDN Security Solution

Automated Cyber Defense enabled by software defined networking

Cyber-attacks are growing in sophistication and volume, and causing massive data breaches at organizations 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 enterprises to mount an effective response.

NEC and Fortinet have established a technology partnership to address the above challenges to help organizations effectively secure their deployments. The Fortinet-NEC joint solution provides Software Defined Networking (SDN)-enabled automated cyber defense, which automates and enhances an organization’s ability to protect against cyber-attacks.

Solution Description

NEC’s ProgrammableFlow SDN solutions simplify network operation and increase network visibility, improving service levels by fine-grained control and visibility of network traffic. 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 Fortinet’s FortiGate enterprise firewall platform, 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 the FortiGate firewall for inspection. When the FortiGate firewall 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 or seconds (because of the automation) as opposed to minutes or days if done manually, without affecting other traffic in the network.

Solution Components

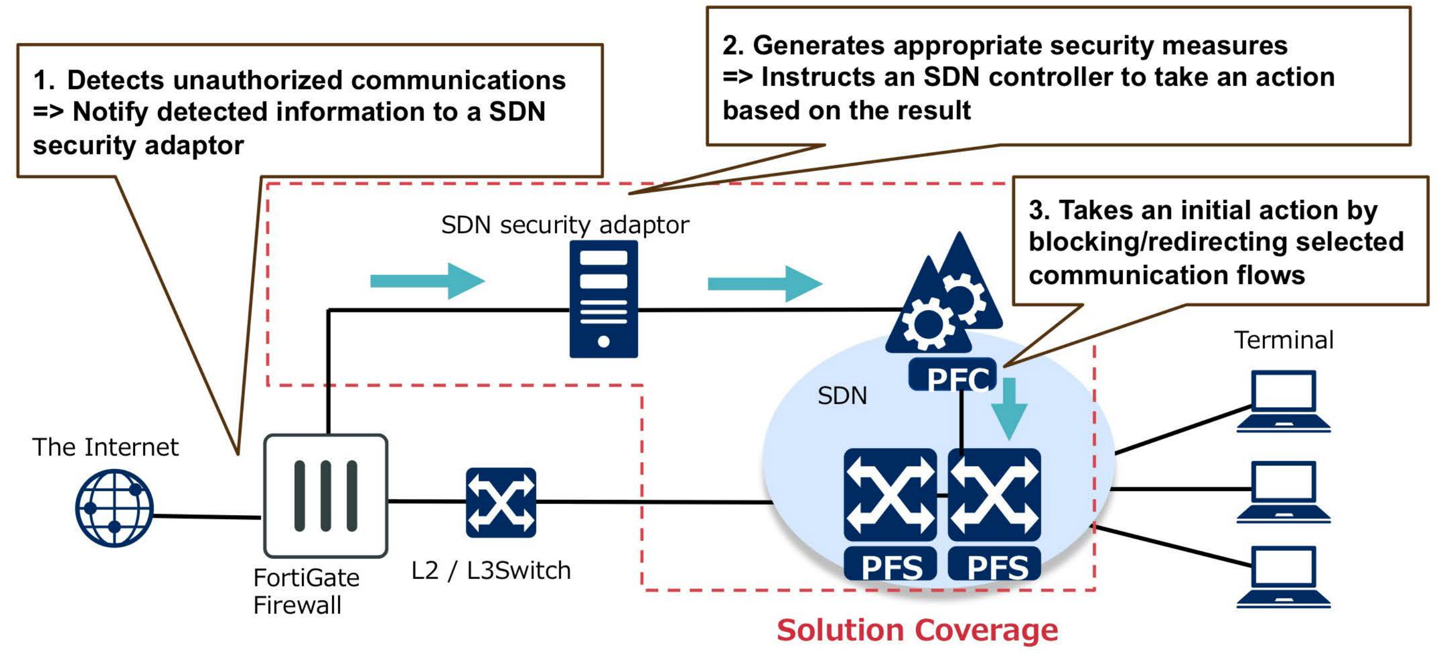
- Fortinet FortiGate firewall (physical or virtual appliance).
- NEC ProgrammableFlow used to control traffic in the enterprise Software Defined Network.
- NEC SDN Security Adaptor used to scan the logs generated by the FortiGate firewall for possible threats, and instructs the ProgrammableFlow controller to block traffic from workstations that show suspicious activity and notifies the system administrator.

Solution Benefits

- Reduces the risk of information leaks, system shut-down, Denial of Service attacks, and ransomware
- Enables faster response to cyberattacks by automatically blocking infected workstations
- Enables enterprise network microsegmentation and uses virtual firewalls between segments, thus confining potential threats
- Allows quick identification of infected workstations
- Enhanced network management by using NEC ProgrammableFlow SDN controller
- Comprehensive end-to-end security visibility provided via the Fortinet Security Fabric
- Leverage the industry’s best validated security protection offered by Fortinet’s FortiGate network security platform to protect against sophisticated cyber-threats

FORTINET
Fabric-Ready

The functionality of the joint solution is summarized in the diagram below.


1. Detects unauthorized communications
=> Notify detected information to a SDN security adaptor
2. Generates appropriate security measures
=> Instructs an SDN controller to take an action based on the result
3. Takes an initial action by blocking/redirecting selected communication flows
SDN security adaptor
The Internet
FortiGate Firewall
L2 / L3Switch
SDN
PFC
PFS
PFS
Terminal
Solution Coverage

- PFC (ProgrammableFlow Controller) / PFS (ProgrammableFlow Switch): NEC SDN appliances
- SDN security adaptor: A system used for connecting between an SDN system and FortiGate firewalls

Figure 1: Solution Architecture.

In summary, NEC SDN automatically blocks communications from an infected terminal when triggered by a security incident detection on the Fortinet FortiGate firewall.

About NEC

Headquartered in Irving, Texas, NEC Corporation of America is a leading technology integrator providing solutions that improve the way people work and communicate. NEC delivers integrated Solutions for Society that are aligned with our customers' priorities to create newvalue for people, businesses and society, with a special focus on safety, security and efficiency. We deliver one of the industry's strongestand most innovative portfolios of communications, analytics, security, biometrics and technology solutions that unleash customers'productivity potential. Through these solutions, NEC combines its best-in-class solutions and technology, and leverages a robust partnerecosystem to solve today's most complex business problems. NEC Corporation of America is a wholly-owned subsidiary of NEC Corporation, a global technology leader with a presence in 160 countries and $28 billion in revenues.

For more information, visit www.necam.com