Samsung SDS

Firewall Monitoring Service

Firewall Monitoring Service to Detect and Respond to Abnormal Firewall Traffic and Worm/ Virus-infected Malicious Traffic

Background

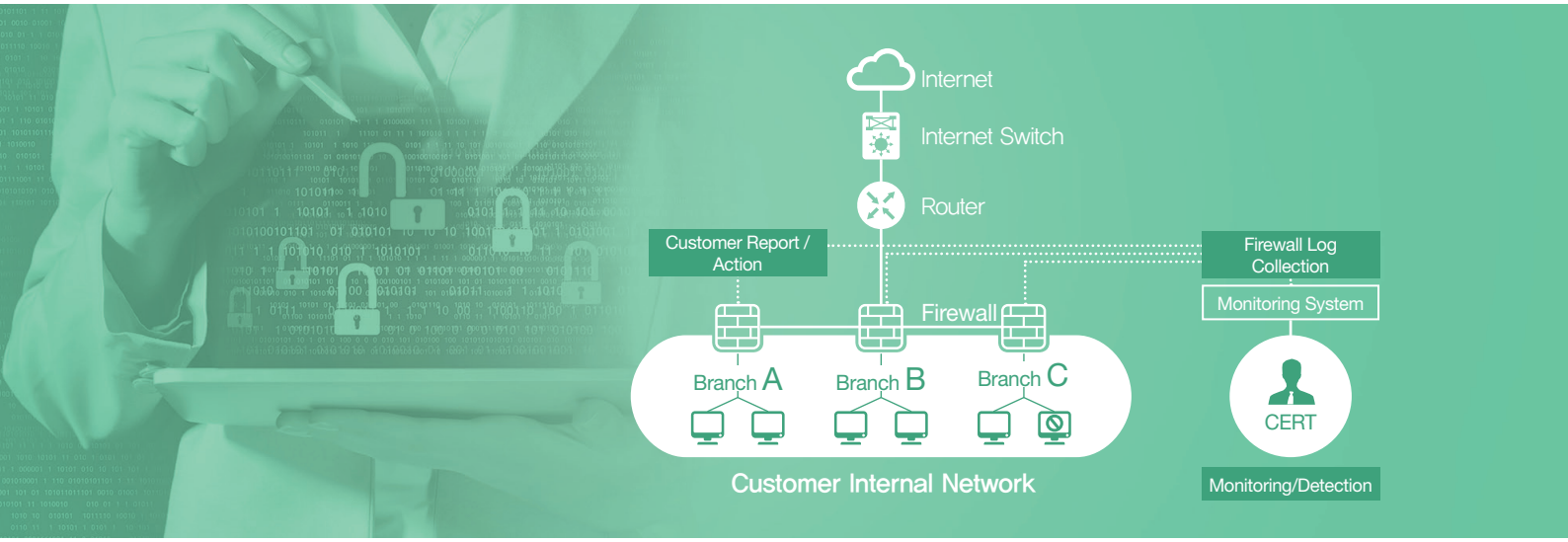
Needs to Cope with Advanced and Diversified Network Threats

Need an advanced firewall monitoring that does more than setting firewall policies and operating equipment. Businesses need a service that detects malicious traffic and analyzes firewall logs

Essential to improve security posture by staying on top of the firewall threat landscape including worm/virus type traffic, abnormally excessive sessions, sudden increase/decrease of firewall sessions and reception failure, etc

Service Overview

A firewall monitoring service that detects and responds to PCs generating malicious traffic such as worm/virus infected traffic or abnormally excessive firewall traffic



Key Features

Real-Time Threat Detection Through Trend & Abnormal Traffic Analysis

- Assess and notify risk levels through usages comparisons on a daily and weekly basis as well as root cause analysis of excessive sessions

Efficient Action and Support Against Detected Threats

- Real time notifications to customers for either emergency or normal case
  - Emergency notification via phone or email of abnormal traffic volume of excessive sessions
  - Warning email whenever a worm/virus-type traffic or any other unique symptom such as log reception failure or firewall abnormality is detected
- CERT analyzes and releases a warning of the source and details of the malicious traffic

Key Services

Worm/Virus Type Malicious Traffic

Detect abnormal traffic that uses the worm/virus generating service port (e.g., IRC[2])

Detection of Abnormally Excessive Sessions

Detect abnormally excessive sessions and their malignity

Detect an application with malfunction traffic

Detection of Firewall Abnormality

Detect a sudden variation of the client's firewall sessions or reception failure

Compare current usage with normal daily/weekly averages

Analyze the root cause for excessive sessions

Classification and Notification of Risk Level of Detected Event

After analyzing the risk level, notify via phone or email any emergency case (e.g., Abnormally excessive traffic) or a warning email of any non critical but potentially threatening symptoms (e.g., Worm/virus type traffic)

Post Management and Results Checking

Request blocking the relevant traffics within the client's firewall and security system

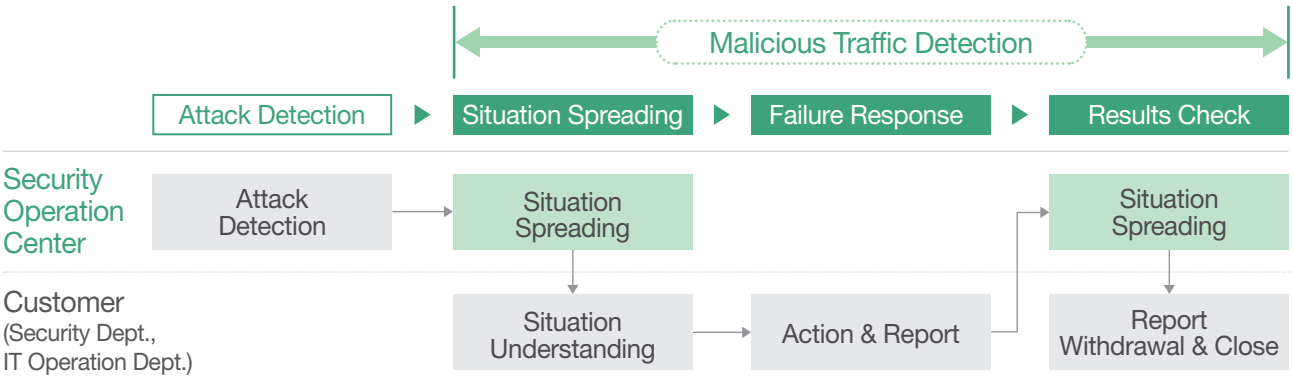
Request taking situational measures including OS security path, vaccine update, etc. and reporting the results

[1] NetBIOS
(Network Basic Input/Output System):
Network regulation created by IBM

[2] IRC (Internet Relay Chat):
A program that facilitates communication on a server networking model

Service Process

Once a malicious traffic is identified, the Security Operation Center and the relevant client's Department run a phased response system based on a standardized process.



SAMSUNG SDS SAMSUNG