4 Best Practices for Using the Cloud to Manage Security
**Introduction**

Next-generation firewalls (NGFWs) secure both on-premises and cloud-based computing infrastructures and are a critical part of a well-designed, defense-in-depth, security architecture. Security professionals depend on NGFWs for visibility, enforcement of security and compliance policies, and to protect their IT infrastructure. Whether your company is large or small, it is important to have tools to easily manage and maintain your firewalls as well as other security devices you may employ.

IT security teams are faced with rapidly evolving threats at every possible point of entry, from the perimeter to the PC and from mobile to the cloud. Fueled by the fast evolution of the threat landscape and changes in network and security architectures, network security management is far more challenging and complex than even a few years ago.

Successful network security management includes security policy management, which incorporates various rules and procedures adopted by network administrators to ensure that unauthorized users do not obtain access. That process makes the network secure and protects and manages network operations. Secondly, a basic change management system must be put in place to ensure backup and recovery of device and security policy configurations. Finally, the management system must support a certain level of threat analysis to understand the risks and vulnerabilities.

![Figure 1: Key elements of network security management.](image)

Security teams must support internal and external compliance mandates, secure new services, optimize performance, ensure availability, and support the ability to troubleshoot efficiently on demand. That’s a lot to balance when managing network security. Small and midsize businesses (SMBs) and managed security service providers (MSSPs) supporting SMB customers need a simple management tool to deploy, manage, and operate network security. The following are key considerations:

**#1 Network Security Management Requires a Macro View**

SMBs need a holistic but easy-to-digest view of their network. With different users and disparate devices like firewalls, access points (APs), switches, etc., SMB IT managers need a normalized view of the network, including configuration of devices, log files, audit trails, security event tracking, traffic analysis, and websites accessed.
With a holistic view of the security infrastructure, security managers can see top threats, top application traffic, top websites and other pertinent information. A networkwide visualization tool is also a critical diagnostic tool, providing analysis that is only possible when considering an overall view. For example, one can use this macro view to see how applications accessed by users may be contributing risk factors, etc.

This macro view should therefore provide quick insights into everything that is happening on the network and empower IT managers to discover, interpret, and prioritize security risks. Additionally, it could highlight the SMB deployment’s security score in comparison against industry average, range, and more.

#2 Device Management Requires a Micro View

Although the macro view is needed to see how all the pieces of network security fit together, network administrators must also be able to look into the details for a particular device, easily accessing high-level information on access policies, routes, interfaces, etc. And this information must be considered within the framework of the broader network, including context such as segments or zones, routers, APs, and switches.

Information must be provided in a digestible fashion. The network components that impact the security device will undoubtedly need to be addressed by administrators by streamlining rule sets. For example, administrators need to be able to block or limit access by application and view violations of these access policies.

Logging into devices on the network for a daily or weekly review is unattainable with a manual process, and less frequent reviewing of device configurations puts both network security and compliance at risk. Cloud-based management with a broad view helps ensure compliance and consistency and reduces the burden on IT resources.

#3 Configuration Backup Is Essential

Once a network is secured and compliant, a secure and easy process to back up configuration files is needed to ensure high availability and uptime even when updates or changes go wrong. A secure configuration backup system allows administrators to automatically store previous configurations of managed firewalls and to make it easy to roll back the configuration to the last known good state.

Rolling back to a previously verified configuration backup enables administrators to recover operations and gain time to troubleshoot configuration changes that may have caused unintended consequences. A configuration backup system that automatically stores known and validated configurations is therefore critical for business continuity.

For example, with a configuration backup system, you can roll back to a secure state and reduce exposure to vulnerabilities, when a new firewall configuration change opens access to risky services, or when there is an unauthorized access path from a partner to an internal zone. Additionally, it can be used to recover operations in case of device failures caused by bad configuration changes.

#4 Log Retention Is Critical

Security needs to be thought of as not an on/off switch but as a process requiring continuous improvement. This requires visibility into network and user behavior, dashboards showing the status of security devices, and detailed logs of security events and changes. However, log retention, though an integral part of any security and compliance program, is often an afterthought. After all, security logs can grow rapidly and administering a separate storage system is expensive, which can impact network and application performance, and requires trained staff.

An effective security management system should automatically retain logs of all security events. In many industries, retaining this information is required for compliance purposes. But whether or not log retention is required, it is always a good idea. After all, should a security incident occur, investigators, insurance companies, and internal procedures will require a forensic examination of the incident. In the event of a forensic investigation, security logs will serve as the primary source of evidence—and the investigation will likely fail if logs are not retained.
The point is that any cloud-based security management system should retain logs for at least a year—and should have the ability to archive logs for far longer.

**How Can Fortinet Help You?**

You need a solution that’s as easy as “ready, set, go” to secure your SMB enterprise. That starts by leveraging a familiar and trusted vendor that offers leading firewall and threat protection solutions to consolidate, simplify, and streamline the security management of your deployment. The solution you select should also be backed by a leading threat research lab and should offer threat feeds for malware detection, intrusion prevention, web filtering, and more.

FortiCloud is the Fortinet Security-as-a-Service family of products powered by a common cloud service delivery platform that offers a common user experience. Part of the FortiCloud suite, FortiGate Cloud is a security management offering available as Software-as-a-Service (SaaS) for deploying, provisioning, and managing Fortinet FortiGate physical and virtual devices. FortiGate Cloud is a simple, secure, and cost-efficient cloud-based management platform for your FortiGate Unified Threat Management (UTM) devices. FortiGate Cloud can be used to manage UTM features and software-defined wide-area networking functionality on FortiGates as well the ability to manage basic FortiAP functions. It offers rich analytics and actionable reports in addition to zero-touch deployment, security log management, and configuration management.

FortiGate Cloud is available to customers as a free subscription or a paid subscription. The free subscription provides visibility, basic reporting, and limited log retention (rolling) as well as the capability to deploy configuration for a very limited number of times (three). After the third configuration deploy attempt, customers will need to upgrade to the FortiGate Cloud paid subscription license.

The paid subscription offers great value to customers through unlimited configuration deployments, backup configuration, custom reporting, one year of customized log retention, and support. See below for a comparison of the capabilities between the two levels of subscriptions.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Free</th>
<th>Paid Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic and application visibility</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Hosted log retention</td>
<td>7 days</td>
<td>1 year</td>
</tr>
<tr>
<td>Cloud provisioning</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Predefined reports</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Configuration management</td>
<td>Limited to 3 deploys</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Customized log retention</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Figure 4: Subscription levels and supported capabilities.

A FortiGate Cloud paid subscription can enable your business to get network security up and running quickly in remote sites, save time and resources, and reduce significant capital investments on on-premises solutions while providing full visibility and reducing risks.