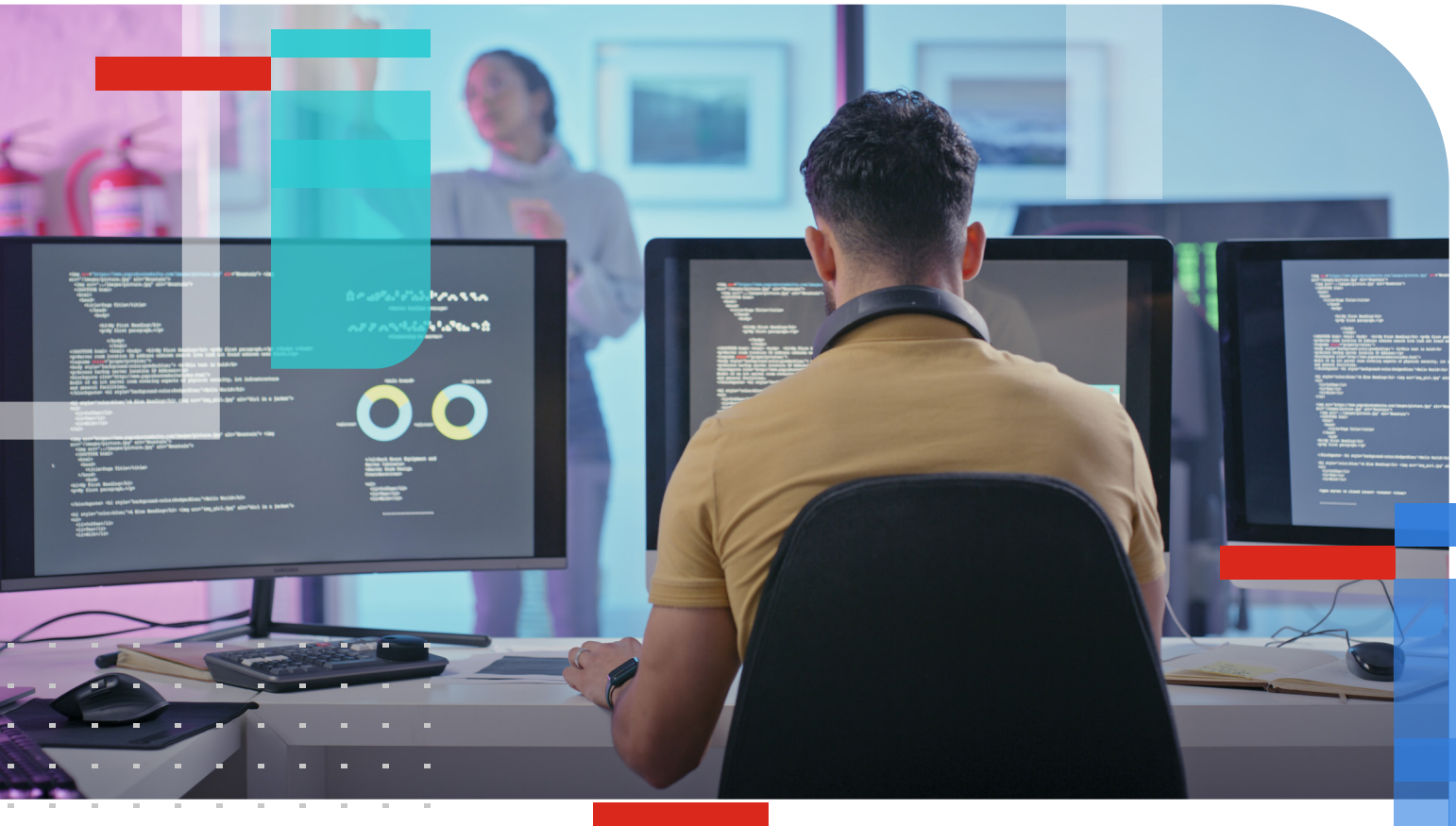
WHITE PAPER

4 Best Practices for Using the Cloud to Manage Security



Executive Summary

Next-generation firewalls (NGFWs) secure on-premises and cloud-based computing infrastructures. They are critical to 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 infrastructures. Whether your organization is large or small, it is important to have tools to easily manage and maintain your firewalls and other security devices you may employ.

IT security teams face 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 threat analysis to understand the risks and vulnerabilities.

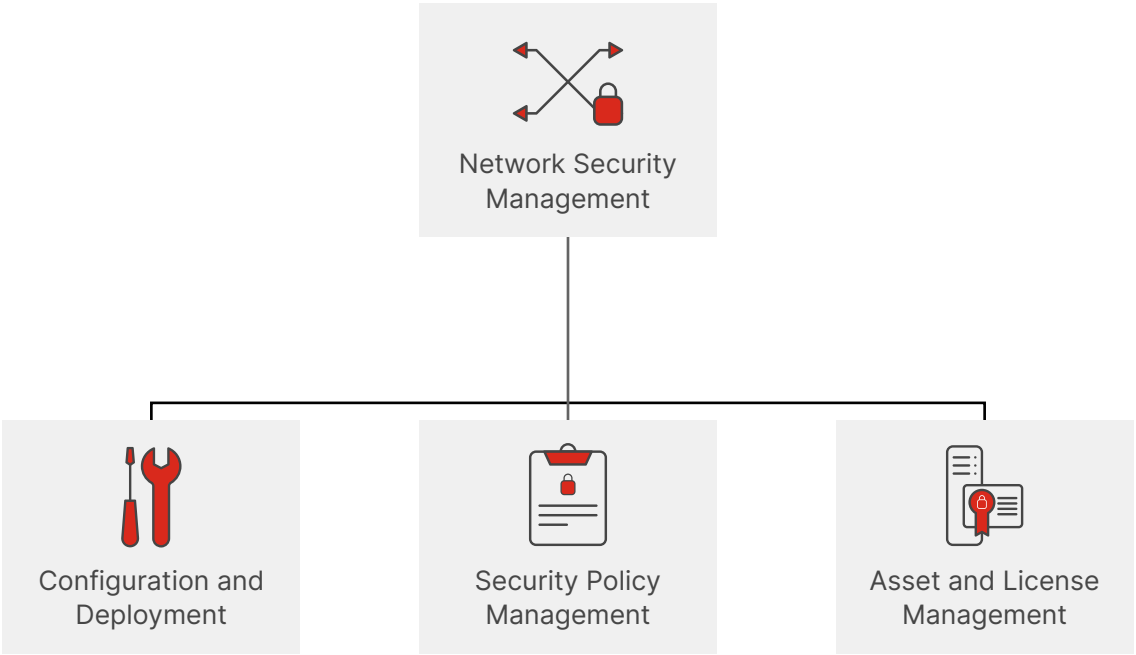


Figure 1: Key elements of network security management

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. Below are four primary considerations:

#1: Network Security Management Requires a Macro View

SMBs need a holistic but easy-to-digest view of their networks. With different users and disparate devices like firewalls, access points (APs), switches, and more, IT managers need a normalized view of the network, including the configuration of devices, log files, audit trails, security event tracking, traffic analysis, and websites accessed.

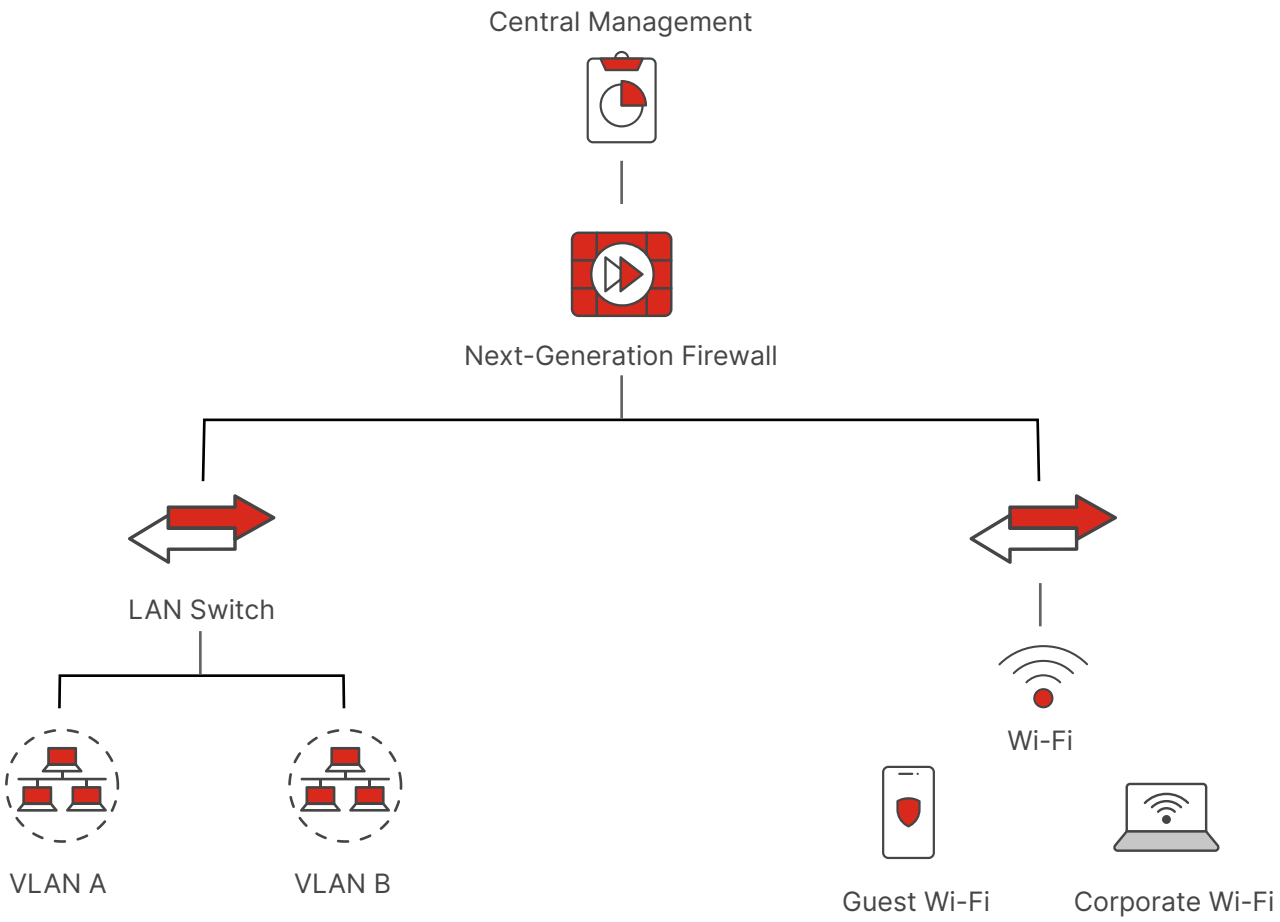


Figure 2: Network macro view

With a holistic view of the security infrastructure, security managers can see top threats, application traffic, websites, and other pertinent information. A networkwide visualization tool is also critical, 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 to risk factors and more.

Therefore, this macro view should provide quick insights into everything 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 to the 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 of a particular device, easily accessing high-level information on access policies, interfaces, and more. This information must be considered within the framework of the broader network, including contexts such as segments or zones, routers, APs, and switches.

The information must be provided in a digestible fashion. Administrators must undoubtedly address the network components that impact the security device via 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 in to devices on the network for daily or weekly reviews is unattainable with manual processes, 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.

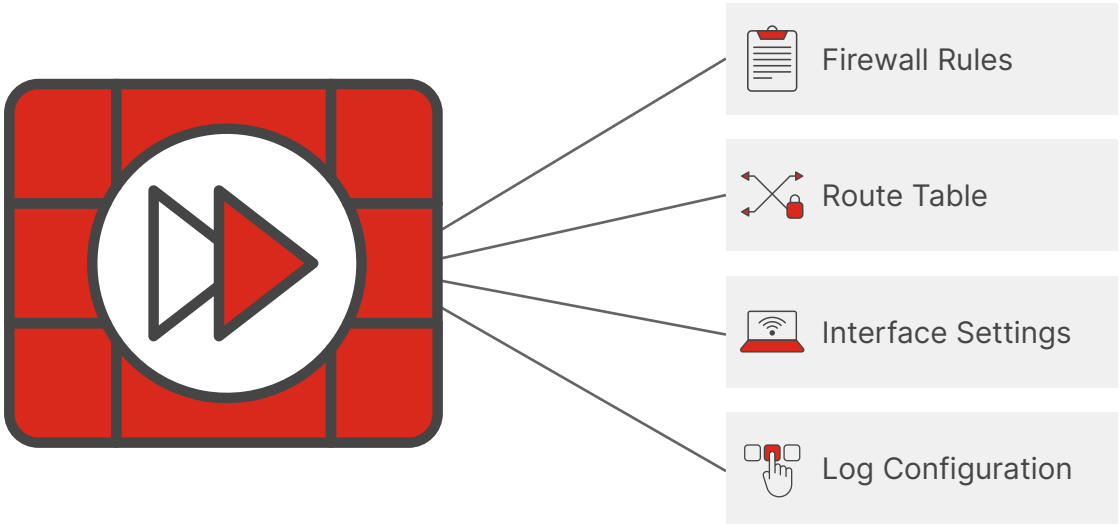


Figure 3: Micro-level view

#3: Configuration Backup Is Essential

Once a network is secured and compliant, a safe 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 considered not an on or 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, 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, impacting 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.

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 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. A leading threat research lab should back the solution you select and 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 uniform user experience. FortiGate Cloud is part of the FortiCloud suite and is a network and security management offering available as Software-as-a-Service (SaaS).

FortiGate Cloud is a simple, secure, and cost-efficient cloud-based management platform that improves operational efficiency by simplifying the initial deployment, setup, and ongoing management of NGFWs and downstream connected devices (like FortiAP, FortiSwitch, and FortiExtender) and SD-WAN with zero-touch provisioning across your branches and sites.

FortiGate Cloud also provides real-time and historical visibility of traffic analytics and security threats to detect and reduce security risks and improve security posture along with actionable reports. This SaaS service is available with FortiGate NGFW devices and virtual machines.

The FortiGate Cloud subscription version offers excellent value to customers through full remote access, unlimited configuration deployments, backup configuration, custom reporting, one year of customized log retention, and support. While a no-subscription version is available, it provides limited visibility, basic reporting, and limited log retention. See the table below for a comparison of the capabilities between the two versions.

Capability	No Subscription	Subscription
Cloud provisioning	✓	✓
Remote access	Read-only	Full access
Configuration management		Unlimited
Firmware upgrades, scripts, and backups		✓
Web, application traffic, and security threat visibility	7 days	1 year
Hosted log retention	7 days	1 year
Reports	360-degree activity report	Multiple predefined reports
Event automation		✓

Figure 4: Subscription levels and supported capabilities

A FortiGate Cloud 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 in on-premises solutions while providing complete visibility and reducing risks.

Conclusion

IT professionals at SMBs should employ four best practices to manage their security when using the cloud. They should also rely on tools like the Fortinet Security-as-a-Service products to easily manage and maintain their firewalls and other security devices.

January 5, 2024 10:27 AM

732974-B-0-EN