

# Achieving NIST 800-53v5 Compliance with FortiGate: An Implementation Guide


Jake Williams


A SANS Implementation Guide

# Achieving NIST 800-53v5 Compliance with FortiGate: An Implementation Guide

## (Companion Paper to "Architecting for Compliance: A Case Study in Mapping Controls to Security Frameworks")

Written by **Jake Williams**

February 2021

*Sponsored by:*

**Fortinet**

Just prior to creating this implementation guide, SANS performed a product review of the FortiGate appliance.[1] During the review, SANS identified multiple features that are useful in achieving compliance with NIST 800-53v5 controls and control families. Although a product review is instrumental in identifying features, it is not an ideal tool for understanding which controls the product supports.

This implementation guide seeks to address this challenge. Because the paper is organized by control family rather than by feature, those considering deploying a FortiGate appliance in their networks can quickly see whether a NIST 800-53v5 control family (or individual control) can be supported through the proposed deployment. For those who have already deployed a FortiGate appliance, this implementation guide can be used as a tool to validate that the organization is getting the best value possible from the deployment.

## NIST 800-53v5 Control Families

The NIST 800-53v5 controls are divided thematically into control families. This implementation guide will address each control family and highlight the expected controls that the FortiGate appliance is likely to be most helpful in supporting for compliance. Some individual controls will be addressed in the paper, specifically where it is not clear how FortiGate will support compliance.

[1] "Architecting for Compliance: A Case Study in Mapping Controls to Security Frameworks," www.sans.org/reading-room/whitepapers/analyst/architecting-compliance-case-study-mapping-controls-security-frameworks-40130

Throughout, the paper will discuss features of the FortiGate appliance that are useful in supporting compliance with the NIST 800-53v5 control family being discussed. In these cases, the feature deep dive will be detailed in only one section (typically where it is first introduced), even if it supports compliance with multiple NIST 800-53v5 controls.

The NIST 800-53v5 control families are as follows:

- Access Control
- Awareness and Training
- Audit and Accountability
- Assessment, Authorization, and Monitoring
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Program Management
- Personnel Security
- Personally Identifiable Information Processing and Transparency
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Supply Chain Risk Management

The remainder of the document describes how FortiGate can support compliance with the NIST 800-53v5 control families. Many of the control families and individual controls listed are not fully addressed by the FortiGate appliance. In some cases, FortiGate is effective only at satisfying the control for FortiGate itself, not for the rest of the customer environment.

## Access Control (AC)

The Access Control family focuses on attributes such as least privilege and access enforcement. The Access Control family intersects with multiple domains, including remote access and wireless access. It includes controls such as session termination and account management.

Access Control can be achieved with the FortiGate product through the use of the following features:

- Account management features
- Logging features
- Customizable HTML pages
- Session management features

Sample controls in the Access Control family addressed by FortiGate include Access Enforcement (AC-3), Information Flow Enforcement (AC-4), Least Privilege (AC-6), Unsuccessful Logon Attempts (AC-7), System Use Notification (AC-8), Session Termination (AC-12), Remote Access (AC-17), and Wireless Access (AC-18).

## Customizable HTML Pages

The system management page contains an option for replacement messages, which allow administrators to reconfigure the FortiGate appliance to display specific messages to respond to events such as failed logins (see Figure 1). These messages specifically address NIST 800-53v5 controls in the Access Control family, such as AC-8 (System Use Notification).

Replacement messages are created using a rich HTML editor built into the FortiGate appliance, as shown in Figure 2.

| | |
|---|---|
| **Authentication (6)** | |
| Device Detection Portal Failure Page | Replacement HTML for device detection portal failure page |
| Email Collection | Replacement HTML for email collection page |
| Email Collection Invalid Email | Replacement HTML for email collection page after user enters invalid email |
| FortiToken Page | Replacement HTML for FortiToken authentication page |
| Login Failed Page | Replacement HTML for authentication failed page |
| Login Page | Replacement HTML for authentication login page |
| **Security (7)** | |
| Application Control Block Page | Replacement HTML for application control block page |
| DLP Block Message | Replacement text for DLP block message |
| DLP Block Page | Replacement HTML for DLP block page |
| FortiGuard Block Page | Replacement HTML for FortiGuard Web Filter block page |
| URL Block Page | Replacement HTML for HTTP URL blocked page |
| Virus Block Message | Replacement text for antivirus block message |
| Virus Block Page | Replacement HTML for antivirus block page |
| **SSL-VPN (2)** | |
| SSL-VPN Login Page | Replacement HTML for SSL-VPN login page |
| SSL-VPN Portal Header | Replacement HTML for SSL-VPN portal page header |

*Figure 1. Replacement Messages*

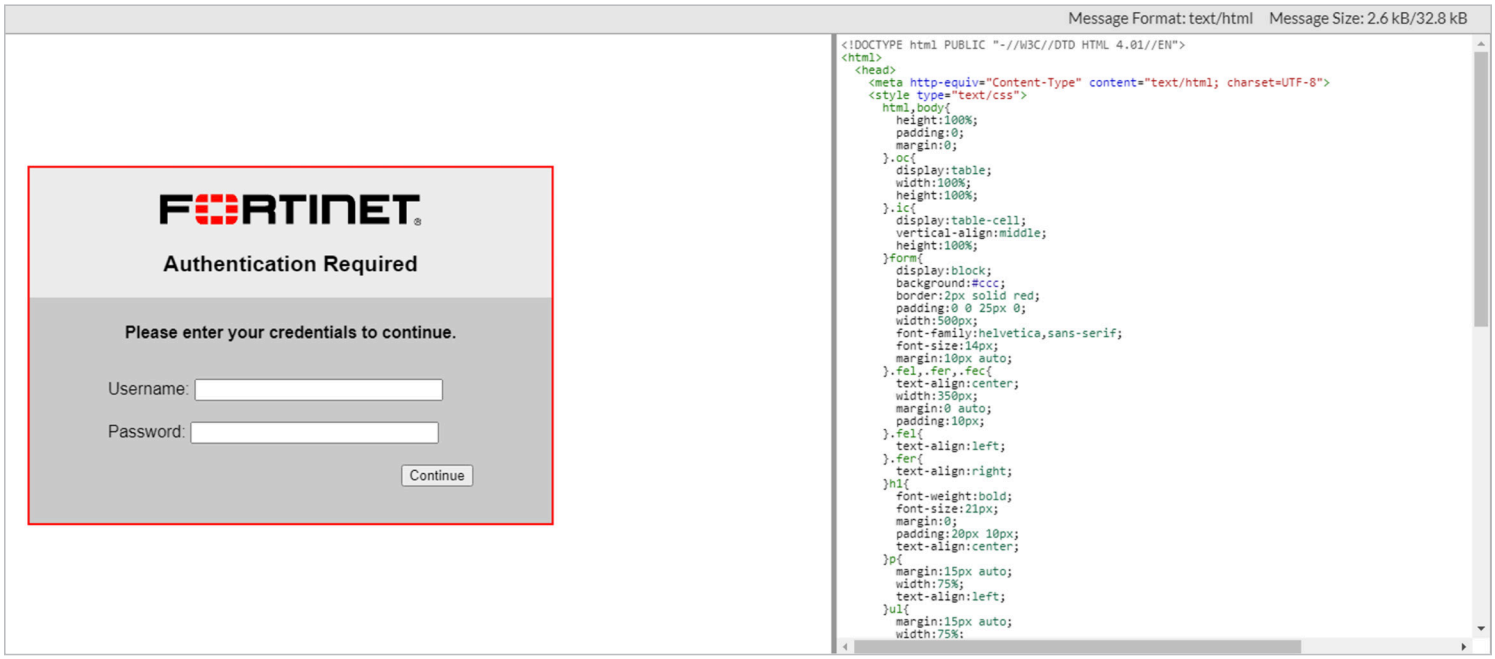


*Figure 2. Replacement Messages Editor*

## Account Management Features

The FortiGate appliance supports multiple types of user definitions. Options include:

- Local user accounts
- Remote Access Dial-In User Service (RADIUS)
- Terminal Access Controller Access Control Service Plus (TACACS+)
- Lightweight Directory Access Protocol (LDAP)
- Fortinet Single Sign-On (FSSO; Fortinet-specific technology)

Creating a new local user begins by specifying the username and password. See Figure 3 for an example.

With a username and password configured, contact information can be specified for the new local user. This configuration supports Short Message Service (SMS)-based multifactor authentication (MFA) in addition to dedicated hardware and software tokens, as shown in Figure 4.

The local user accounts on FortiGate allow a user to be a member of multiple groups. See Figure 5 for an example. Although this should be the norm for any user account system, it is the sort of flexibility that is lacking in far too many systems.

Although many organizations won't use the built-in user management system with FortiGate, it's good to know that it's fully featured enough to meet compliance requirements within NIST 800-53v5.

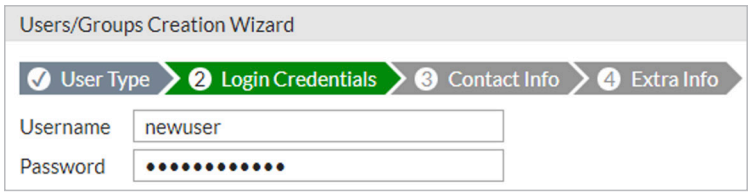


*Figure 3. Local User Creation*

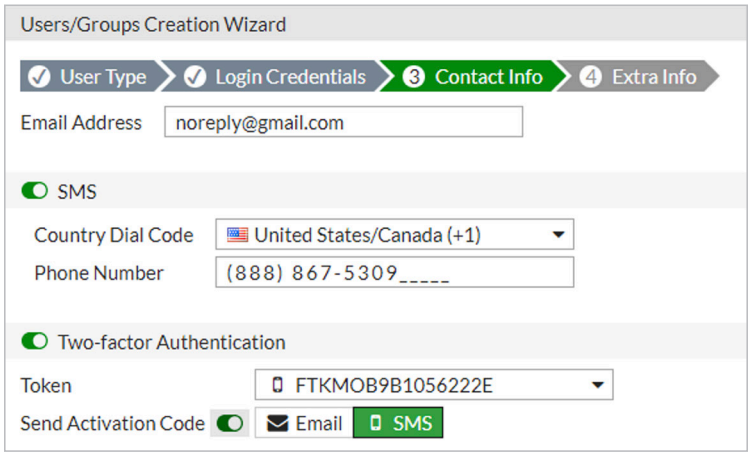


*Figure 4. User MFA Options*

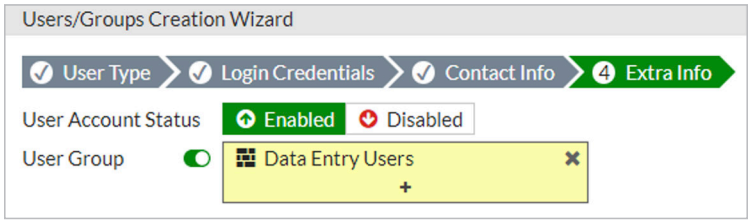


*Figure 5. Group Memberships*

## Awareness and Training (AT)

The Awareness and Training control family includes controls such as Role-Based Training and Training Records that promote security awareness directives within the organization. The FortiGate appliance does not support compliance with any NIST 800-53v5 controls in the Awareness and Training control family.

## Audit and Accountability (AU)

The Audit and Accountability control family includes controls such as Event Logging and Non-Repudiation. The FortiGate appliance is rich in audit features and includes multiple logging and auditing controls, many of which support the Audit and Accountability control family.

Audit and Accountability can be achieved with the FortiGate product through the use of the following features:

- Logging features
- Log forwarding

## Logging Features

FortiGate has no shortage of logging features that support NIST 800-53v5. As shown in Figure 6, logs can be stored (and viewed) locally, though as we'll detail later, they can also be forwarded to other locations.

Add Filter

| # | Date/Time | Level | User | Message |
|---|---|---|---|---|
| 1 | Minute ago | | ladmin | Administrator ladmin logged out from ssh(10.20.30.160) |
| 2 | Minute ago | | ladmin | Administrator ladmin logged in successfully from ssh(10.20.30.160) |
| 3 | Minute ago | | ladmin | Administrator ladmin logged out from ssh(10.20.30.160) |
| 4 | Minute ago | | ladmin | Administrator ladmin logged in successfully from ssh(10.20.30.160) |

*Figure 6. System Log Entry List*

Each log event has details that can be viewed in the details pane, which provides additional information. See Figure 7 for an example.

**General**
Date 2020/12/27
Time 14:31:07
Duration 0s
Virtual Domain root
Log Description Admin logout successful

**Source**
IP 10.20.30.160
Device ID FGR60DTK19000673
User ladmin

**Destination**
IP 10.20.30.1

**Action**
Action logout
Status success
Reason exit

**Security**
Level

**Event**
User Interface ssh(10.20.30.160)
Message Administrator ladmin logged out from ssh(10.20.30.160)

*Figure 7. Log Details*

## Log Forwarding

Logs need not only be stored on the FortiGate appliance. Administrators can configure remote logging as well using the Log Settings menu (see Figure 8). Of particular interest are the options for sending logs in batches. This option can cut down on network traffic because logs will be sent at particular intervals. Although most organizations will probably prefer real-time forwarding of log entries, the option for batch forwarding is particularly attractive for remote offices. If logs are being forwarded to an off-site location (let's say a FortiGate appliance in a remote office is forwarding logs to the central office), the option to batch forward logs is particularly useful. The option to encrypt log entries is also useful and supports both the System and Communications Protection control family and the System and Information Integrity control family (which will be discussed later in this paper).

Log Settings

Local Log
Memory

Remote Logging and Archiving

FortiAnalyzer can also be installed on Amazon Web Services (AWS).
Please watch the setup Video.

Send logs to FortiAnalyzer/FortiManager
Use FortiManager
IP address 10.20.30.31 Test Connectivity
Logging to ADOM lab60
Storage usage 0% 22.58 GiB / 0 B
Analytics usage 0% 19.66 GiB / 0 B (Number of days stored: 48/60)
Archive usage 0% 2.92 GiB / 0 B (Number of days stored: 151/365)
Upload option Real Time | Every Minute | Every 5 Minutes
SSL encrypt log transmission

*Figure 8. Log Settings*

FortiGate displays the usage of particular log types and breaks down the log volume for each type (see Figure 9). This function is useful for administrators considering adjusting their logging posture.

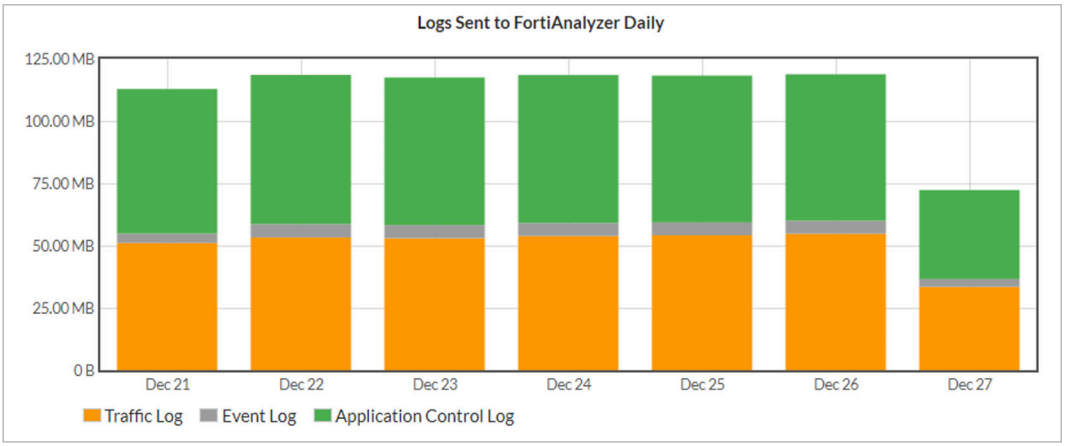


*Figure 9. Log Volumes*

FortiGate also supports the use of Syslog and cloud forwarding using FortiCloud, specifically supporting the Audit Log Storage Capacity (AU-4) control of NIST 800-53v5. See Figure 10 for an example.


*Figure 10. Syslog and FortiCloud*

Unlike many systems, FortiGate doesn't take an all-or-nothing approach to logging. As shown in Figure 11, FortiGate offers multiple options for selecting specifically which logs should be forwarded to the configured logging destinations.

## Assessment, Authorization, and Monitoring (CA)

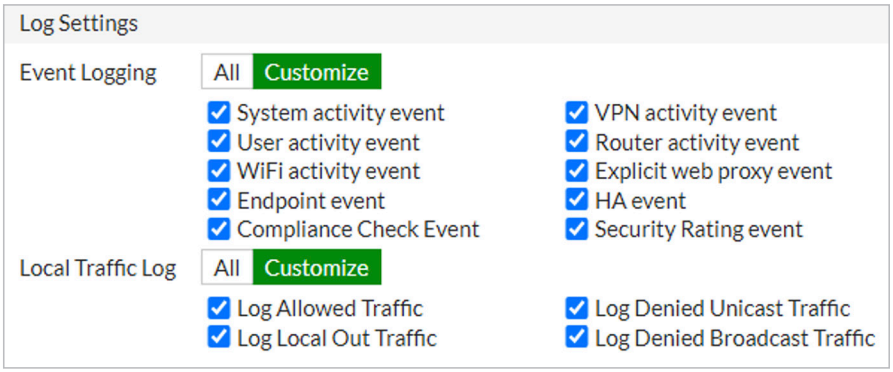


*Figure 11. Log Selection*

The Assessment, Authorization, and Monitoring control family of NIST 800-53v5 mostly focuses on documentation-type activity, such as requirements for penetration testing. Although a properly deployed and configured FortiGate appliance will certainly help with penetration testing results (and more broadly, security certification, now merged with control assessments), those options will not be covered here. The FortiGate appliance most aptly supports the Continuous Monitoring control.

Compliance with the NIST 800-53v5 Assessment, Authorization, and Monitoring control family can be achieved with the FortiGate product through the use of the following features:

- FortiView
- Logging features

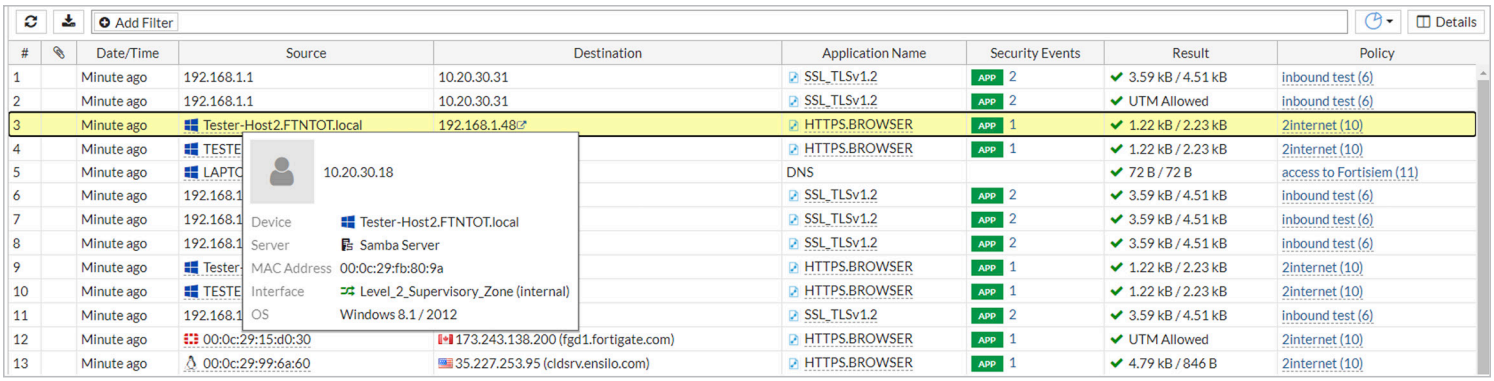


*Figure 12. FortiView*

## FortiView

The traffic log in FortiView supports continuous monitoring (see Figure 12). This support goes far beyond the NetFlow records available with traditional networking products and logs additional information, including:

- MAC address
- Device name
- Service
- OS
- Source and destination byte counts
- Interface on which the traffic was seen

Additional information about the application can be viewed by hovering over the Application Name field, as shown in Figure 13.

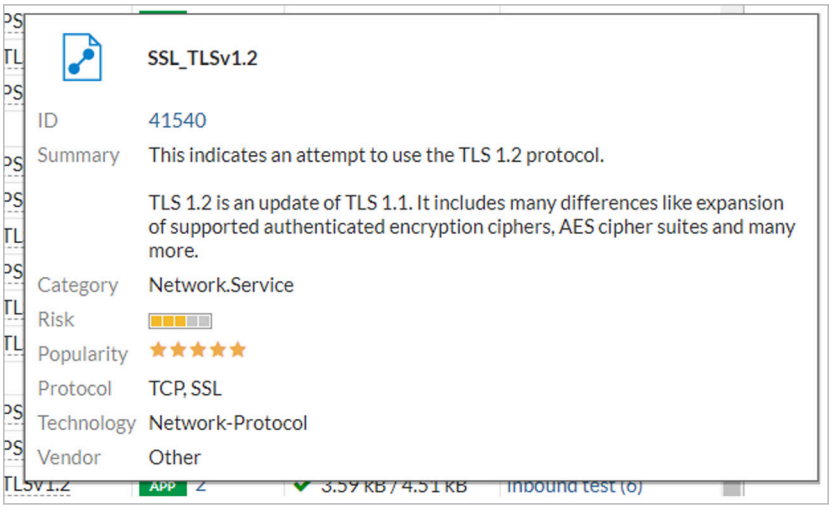


*Figure 13. Application Details*

Additional details are available for any log entry by clicking on the entry, as shown in Figure 14.

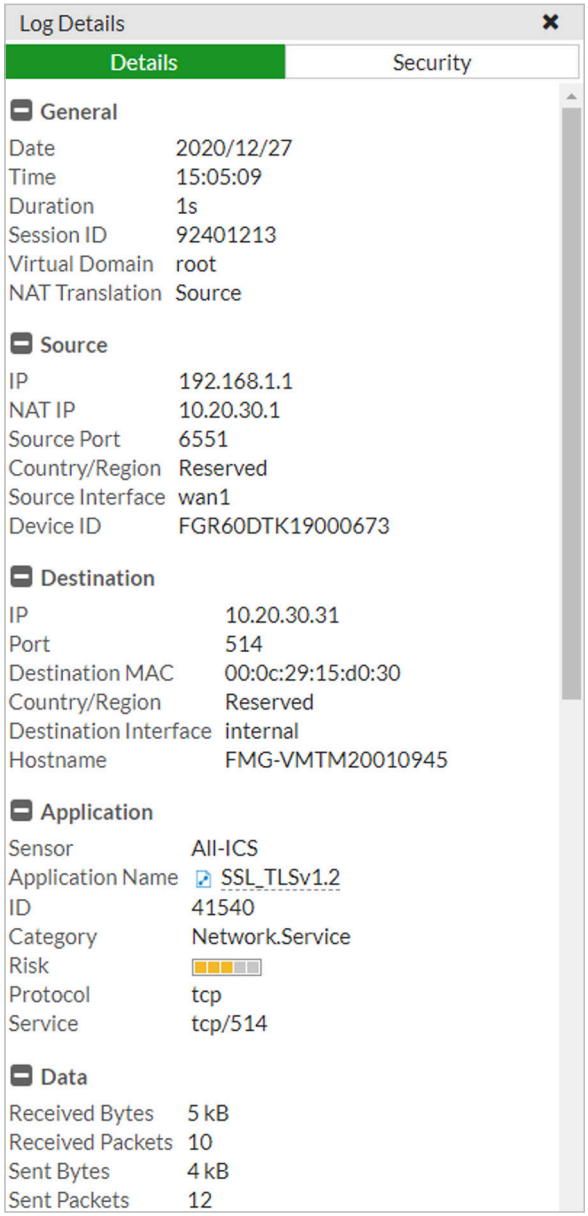


*Figure 14. Log Details*

## Configuration Management (CM)

The Configuration Management control family of NIST 800-53v5 is concerned with the secure configuration of devices. Controls in this family include Least Functionality (CM-7), User-Installed Software (CM-11), and Baseline Configuration (CM-2).

The FortiGate appliance doesn't allow any user-installed software, but it can be used to detect it. Presuming that the organization has a baseline of normally installed software, any user-installed software should show up as anomalous. The Application Control feature supports the detection of applications passing traffic on the network. It goes beyond simply looking at commonly used ports into deep traffic inspection and protocol analysis.

The following FortiGate features support compliance with the Configuration Management NIST 800-53v5 control family:

- Application Control
- Configuration Backup (System menu)
- FortiClient compliance

### Application Control

The Application Control feature of the FortiGate appliance assists with identifying applications based on network traffic inspection. Application Control supports a wide range of applications and separates applications by both category and cloud presence (see Figure 15). Supporting both application and filter overrides proves useful in deploying very granular configurations.

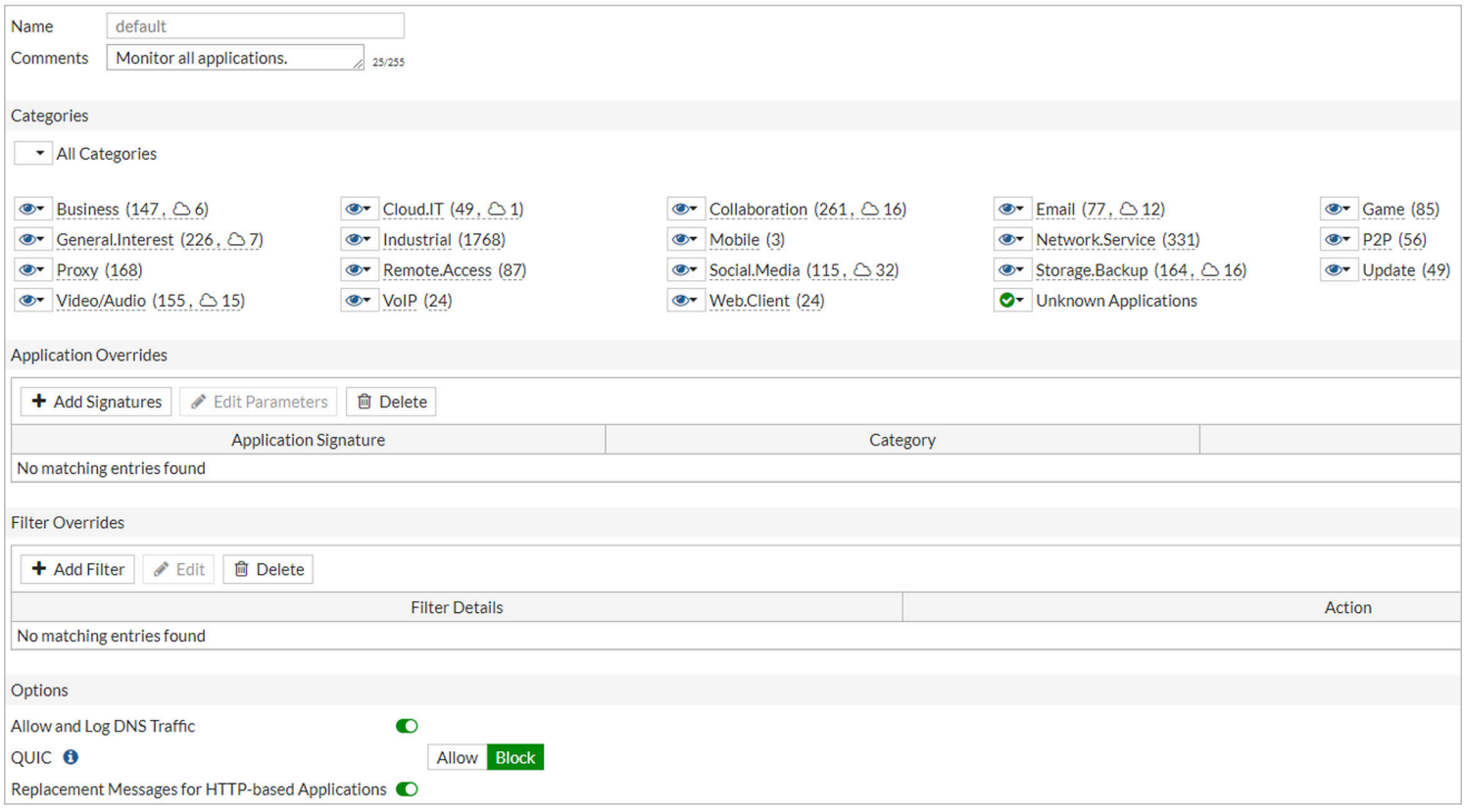


*Figure 15. Application Control Configuration*

### FortiClient Compliance

When configured and deployed, the FortiGate appliance can drive policy for the FortiClient agents deployed on endpoints in the network. As shown in Figure 16, applications can be explicitly blocked by preventing particular process names from running. Alternatively, an SHA256 signature for disallowed applications can be configured.

Additionally, FortiGate supports a security posture check for supported devices. FortiGate supports checking for the following items:

- Real-time protection
- Third-party antivirus on Windows
- Web filter
- Application firewall

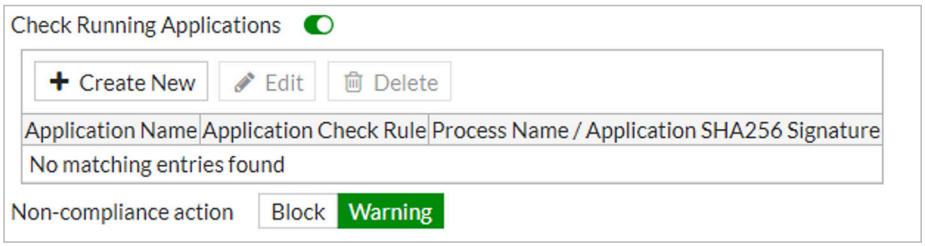


*Figure 16. Running Application Check*

If any of these compliance options are not met, FortiGate can either warn the user or block the device from communicating on the network.

## Contingency Planning (CP)

The Contingency Planning control family of NIST 800-53v5 is concerned with ensuring that the organization can continue to operate during and after an unexpected event. These events include hardware and software failures, security events, or anything that requires the organization to operate in a nonstandard capacity. Controls in this family include System Backup, System Recovery and Reconstitution, Alternate Communication Protocols, Safe Mode, and Alternate Security Mechanisms.

The following features of the FortiGate appliance support the NIST 800-53v5 Contingency Planning control family:

- Application Control
- Multiple protocols for administration
- FortiGate Configuration Backup and Recovery

FortiGate supports system backup and recovery to a defined configuration, ensuring that the appliance aligns with the controls. However, adoption of FortiGate does not satisfy the overall intent of the System Backup (CP-9) and System Recovery and Reconstitution (CP-10) controls for the broader organization.

In many environments, the deployment of a FortiGate appliance will contribute to a defense in depth model. In these cases, it is expected that some overlaps in capabilities will exist between FortiGate and other security controls deployed in the environment. In those cases, FortiGate will support the Alternate Security Mechanisms control (CP-13). Whether FortiGate performs these functions on a normal basis or is employed only when another security control is unavailable (for instance, due to a hardware failure on a dedicated IPS), FortiGate can supply overlapping coverage for a number of security controls, including but not limited to:

- Application Control (aka Application "Whitelisting")
- Network Monitoring
- Intrusion Detection/Prevention
- Device Inventory
- Wireless Intrusion Prevention
- Inter-VLAN Network Access Control
- VPN Services
- AAA Services

The Alternate Communications Protocols control (CP-11) requires that the organization have multiple protocols available to maintain continuity of operations. The FortiGate appliance assists in compliance by both supporting multiple protocols for administration of the device itself and filtering communications protocols (such as telnet) that are seen as an unacceptably high risk.

## Identification and Authentication (IA)

The Identification and Authentication control family of NIST 800-53v5 is concerned with performing positive identification of a user and securely authenticating that user. In addition to permanent employees, the Identification and Authentication control family requires organizations to consider how they will handle these operations for:

- Permanent users
- Temporary employees and contractors
- Guests
- Nonhuman users (e.g., service accounts)

FortiGate can also authenticate devices, supporting Device Identification and Authentication (IA-3).

The following features of the FortiGate appliance support the NIST 800-53v5 Identification and Authentication control family:

- Account management features
- FortiToken management (MFA)
- Application Control
- Firewall features

Many controls in the NIST 800-53v5 Identification and Authentication control family can be addressed partially or completely through the use of a FortiGate appliance, depending on organizational needs. For instance, Authenticator Management (IA-5) can be addressed through FortiToken Management features (if configured). Device Identification and Authentication (IA-3) can be accomplished through the use of FortiClient (in some configurations).

Firewall and Application Control features can assist in ensuring that only approved protocols are used for authentication in the network.

The degree to which the deployment of a FortiGate appliance will achieve compliance with Identification and Authentication will depend on the organization's specific needs and other products/architecture already in place.

## Incident Response (IR)

The Incident Response control family of NIST 800-53v5 is concerned with dictating the requirements for proactive plans around addressing security incidents. The FortiGate appliance does not assist with most of the controls within the NIST 800-53v5 Incident Response control family because most relate to planning and testing rather than the response itself.

However, the following features of FortiGate will assist in compliance with the Information Spillage Response (IR-9) control:

- FortiView
- Firewall features
- Intrusion prevention systems (IPS) features
- Data loss prevention

A specific requirement of the control is that organizations have a plan to isolate the contaminated system or system component. This isolation can be achieved by using FortiGate's firewall features. Another requirement is identifying other systems or system components that may have been subsequently contaminated. Depending on the type of information spillage, it is likely that FortiView can assist in understanding additional systems to which the information was spilled. The IPS features of FortiGate may also be useful in preventing additional spillage.

## Maintenance (MA)

The Maintenance control family of NIST 800-53v5 is concerned with performing maintenance on information systems and system components to prevent security issues. The FortiGate appliance does not meaningfully contribute to compliance with the NIST 800-53v5 Maintenance control family.

## Media Protection (MP)

The Media Protection control family of NIST 800-53v5 is concerned with inventory, labeling, and protection of physical media used to support information systems operations. The FortiGate appliance does not meaningfully contribute to compliance with the NIST 800-53v5 Media Protection control family.

## Physical and Environmental Protection (PE)

The Physical and Environmental Protection control family of NIST 800-53v5 is concerned with ensuring that physical workspaces have appropriate physical security controls and that things such as emergency lighting and power are in place. The FortiGate appliance does not meaningfully contribute to compliance with the NIST 800-53v5 Physical and Environmental Protection control family.

## Planning (PL)

The Planning control family of NIST 800-53v5 is concerned with security planning and documentation. The FortiGate appliance does not meaningfully contribute to compliance with the NIST 800-53v5 Planning control family.

## Program Management (PM)

The Program Management control family of NIST 800-53v5 is concerned with building security programs and governance. The FortiGate appliance doesn't directly contribute to specific Program Management controls; however, many FortiGate features can contribute to detecting and remediating security concerns mandated in the NIST 800-53v5 Program Management control family. The following FortiGate features are useful in achieving compliance with Program Management controls:

- FortiView
- Application Control
- Firewall features
- FortiClient Compliance

The NIST 800-53v5 Program Management control family requires the implementation of an Insider Threat Program (PM-12). One of the key mechanisms useful in the early detection of insider threats is discovering the use of unsanctioned applications. FortiView, Application Control, and FortiClient Compliance (application whitelisting) can all assist with the detection of insider threats using unsanctioned applications.

System Inventory (PM-5) is a challenge that probably won't be addressed by FortiGate alone, but the system inventory features of FortiGate can contribute to compliance with this control. The degree to which FortiGate contributes to the control depends on the network architecture used at the organization. The Enterprise Architecture (PM-7) requirement is also supported by FortiGate, though obviously FortiGate won't account for an entire enterprise security architecture.

## Personnel Security (PS)

The Personnel Security control family of NIST 800-53v5 is concerned with the selection, screening, hiring, and termination of employees. The FortiGate appliance does not meaningfully contribute to compliance with the NIST 800-53v5 Personnel Security control family.

## Personally Identifiable Information Processing and Transparency (PT)

The Personally Identifiable Information Processing and Transparency control family of NIST 800-53v5 is concerned with policies for processing personally identifiable information (PII) and providing required notifications that PII is being collected and/or processed. It may seem counterintuitive, but the FortiGate appliance does not meaningfully contribute to compliance with the NIST 800-53v5 Personally Identifiable Information Processing and Transparency control family. Skeptics might note that there are strict requirements for processing PII that include authentication and secure transmission. However, this control family is focused on policies for processing PII rather than the controls used to protect the PII itself. The controls used to protect PII are covered in other sections of NIST 800-53v5.

## Risk Assessment (RA)

The Risk Assessment control family of NIST 800-53v5 is concerned with assessing risks and impacts within the organization. Although risk assessment is mostly a planning activity, vulnerability management and threat hunting (both of which FortiGate helps with) are included in this control family. The following FortiGate features are useful in achieving compliance with Risk Assessment controls:

- DNS logging
- FortiClient Compliance
- FortiView
- Application Control
- URL filtering

FortiClient Compliance features support the identification of unpatched vulnerabilities on the endpoint, assisting in compliance with Vulnerability Monitoring and Scanning (RA-5). See Figure 17 for detail. Although most organizations will probably use a purpose-built enterprise vulnerability scanner, reliance on FortiClient is also helpful. Note, however, that FortiClient will not perform network vulnerability scans. FortiClient provides defense in depth, a requirement highlighted throughout NIST 800-53v5.

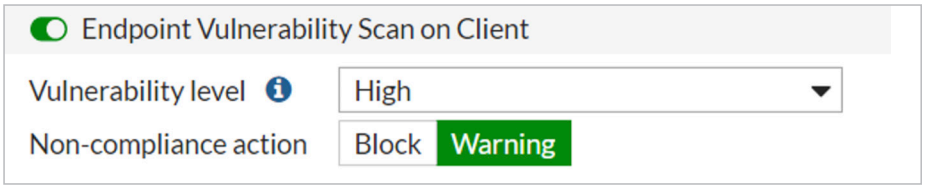


*Figure 17. FortiClient Vulnerability Management*

Vulnerability Monitoring and Scanning (RA-5) will also be aided by FortiView and Application Control. Because the FortiView interface logs known information about an endpoint, including OS version, it may be useful in identifying devices that are running unsupported operating systems. Additionally, Application Control may discover applications that are no longer vendor supported, or at least are unsupported by the organization's vulnerability management program. Even the combination of these features is not a replacement for a robust vulnerability scanning solution, however, so organizations should use all tools at their disposal on a problem as critical as vulnerability management.

FortiGate contributes to the Threat Hunting (RA-10) control through the use of FortiView, URL filtering, and DNS logging. FortiView can be used to highlight communications that are indicative of malware beaconing or data exfiltration activity.

### URL Filtering

As presented in Figure 18, URL filtering can be configured to block access to specific patterns indicative of attacker activity. For instance, many command and control (C2) control panels use specific patterns in their URLs. If the organization receives threat intelligence about the characteristics of these C2 panels, it may configure blocking actions for the URL patterns. Alternatively, it may choose to implement monitoring rules to mitigate potential false positive detections.

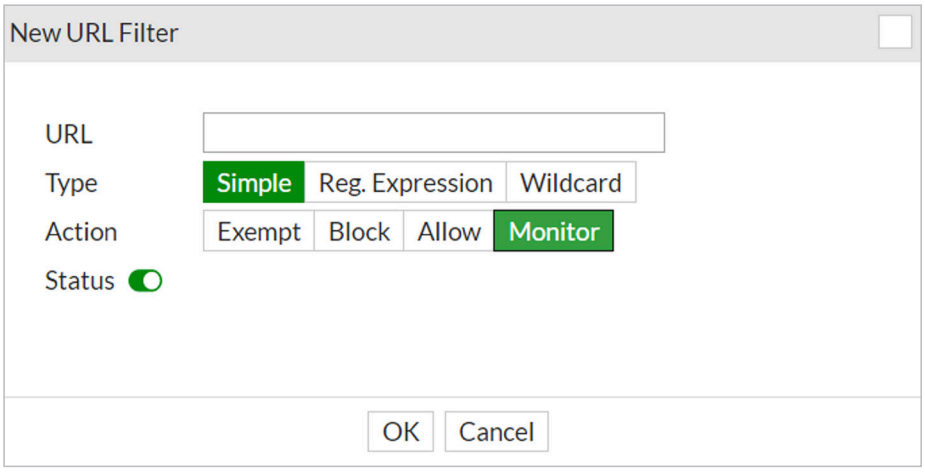


*Figure 18. URL Filtering*

### DNS Logging

DNS logs are critical in any threat hunting operation. The FortiGate appliance natively supports logging all DNS requests and responses. It is critical that FortiGate offers this feature because even today, organizations are still running DNS servers for which logging is extremely hard to configure and/or resource-intensive to enable. See the SANS product review companion paper, "Architecting for Compliance: A Case Study in Mapping Controls to Security Frameworks," for more detail on the DNS logging use case.

## System and Services Acquisition (SA)

The System and Services Acquisition control family of NIST 800-53v5 is concerned with the secure acquisition of hardware, software, and services. Additionally, this control family addresses the security of developers and developer awareness training. The FortiGate appliance does not meaningfully contribute to compliance with the NIST 800-53v5 Systems and Services Acquisition control family.

## System and Communications Protection (SC)

The System and Communications Protection control family of NIST 800-53v5 is concerned with assessing risks and impacts within the organization. There are 51 individual controls in the System and Communications Protection control family, and many of them can be addressed by FortiGate fully or in part. As a result, an entire paper could be written on the FortiGate features used to comply with individual controls in the System and Communications Protection control family. For the sake of space considerations, we note that FortiGate can assist with the following controls under this family and leave the implementation specifics for a later work.

As an example control within the SC family, Boundary Protection (SC-7) is facilitated by FortiGate. Figure 19 shows the Security Fabric visualization, which can be viewed in both physical and logical topologies, enhancing the analyst's understanding of the network.

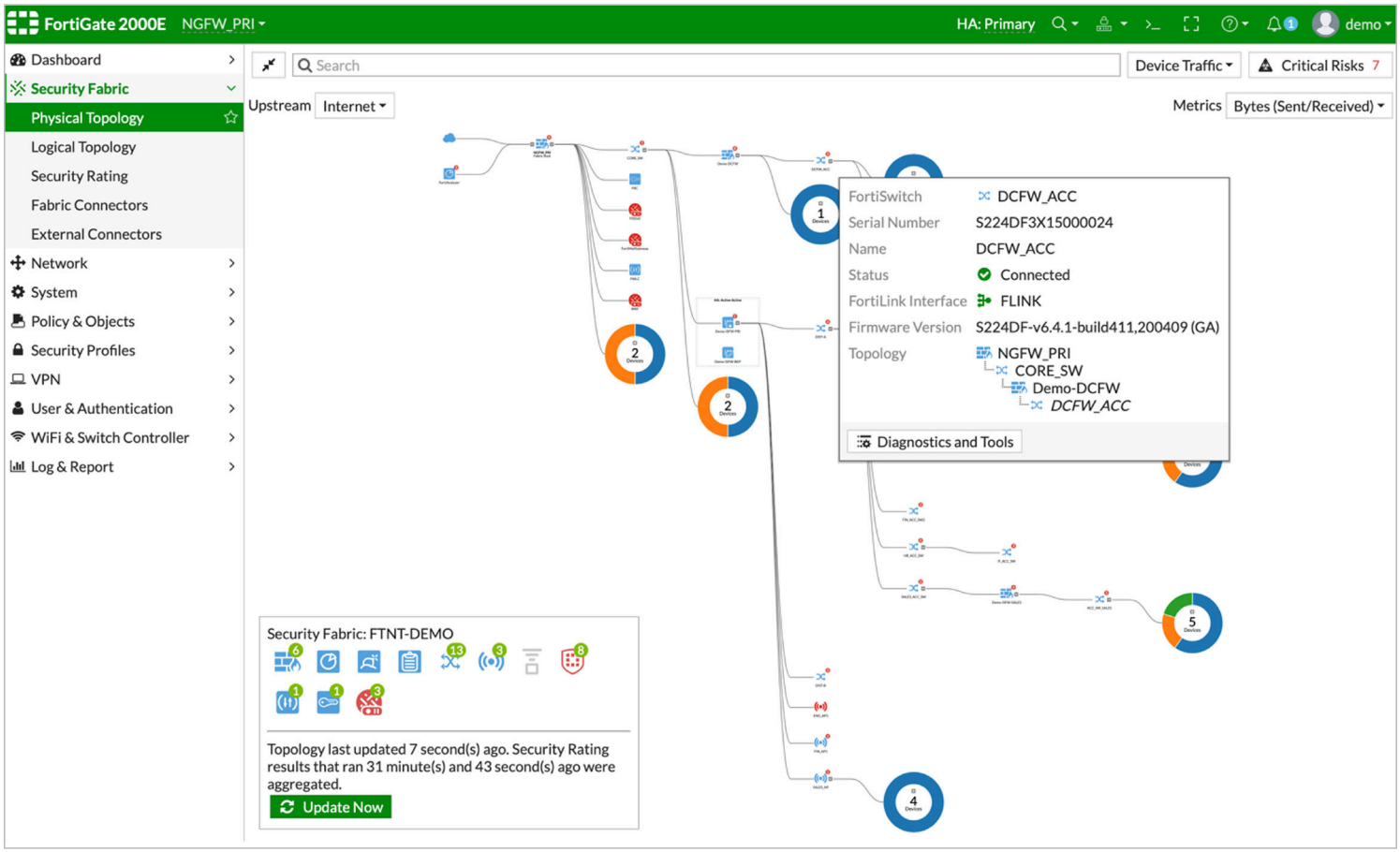


*Figure 19. Security Fabric*

FortiGate implementations partially or fully satisfy the following controls in the System and Communications Protection family:

- Separation of System and User Functionality (SC-2)
- Security Function Isolation (SC-3)
- Denial-of-Service Protection (SC-5)
- Resource Availability (SC-6)
- Boundary Protection (SC-7)
- Transmission Confidentiality and Integrity (SC-8)
- Network Disconnect (SC-10)
- Cryptographic Key Establishment and Management (SC-12)
- Cryptographic Protection (SC-13)
- Collaborative Computing Devices and Applications (SC-15)
- Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21)
- Session Authenticity (SC-23)
- Fail in Known State (SC-24)
- Heterogeneity (SC-29)
- Concealment and Misdirection (SC-30)
- Non-Modifiable Executable Programs (SC-34)
- External Malicious Code Identification (SC-35)
- Out-of-Band Channels (SC-37)
- Wireless Link Protection (SC-40)
- Usage Restrictions (SC-43)
- System Time Synchronization (SC-45)
- Cross Domain Policy Enforcement (SC-46)
- Alternate Communications Paths (SC-47)
- Sensor Relocation (SC-48)
- Software-Enforced Separation and Policy Enforcement (SC-50)
- System Partitioning (SC-32)

## System and Information Integrity (SI)

The System and Information Integrity control family of NIST 800-53v5 is concerned with preventing threats to the integrity of data and the systems processing it. Although related, this differs from the System and Communications Protection control family in that the SI family does not address the confidentiality of communications and data. The following FortiGate features are useful in achieving compliance with SI controls (though many controls will be satisfied only for FortiGate itself):

- Malicious Code Protection (SI-3)
- System Monitoring (SI-4)
- Security Alerts, Advisories, and Directives (SI-5)
- Software, Firmware, and Information Integrity (SI-7)
- Spam Protection (SI-8)
- Information Input Validation (SI-10)
- Error Handling (SI-11)
- Non-persistence (SI-14)
- Memory Protection (SI-16)

### Antivirus Features

FortiGate supports antivirus definitions that can be used on endpoints and mobile devices (see Figure 20). Any security analyst will understand that Windows executables should never be sent as email attachments. Although we would certainly hope that these would be stripped by the mail server, it's easy to appreciate the defense in depth provided by FortiGate in identifying any executable email attachment as malware. Although some may argue that any email with an executable attachment is a phishing email and not spam, this feature definitely helps restrict some spam.

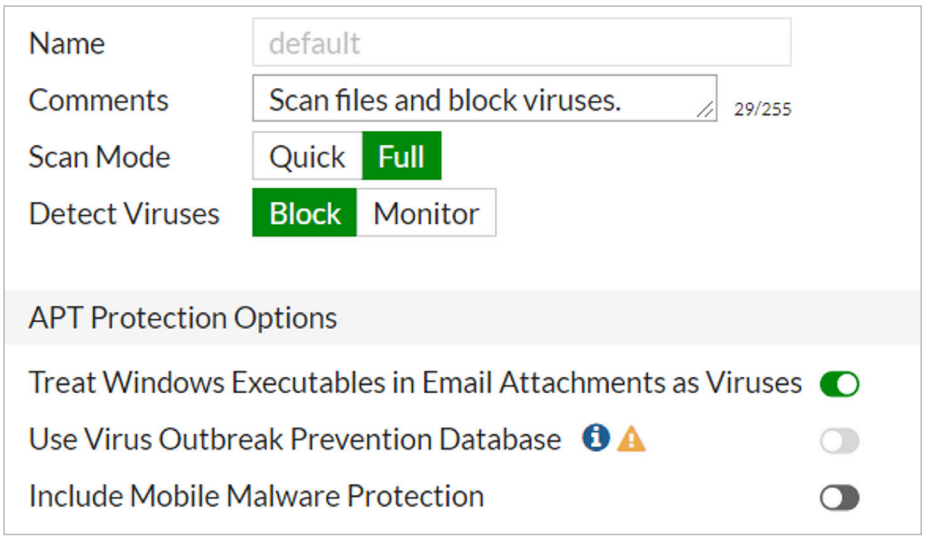


*Figure 20. Antivirus Configuration*

The FortiGate antivirus feature also supports compliance with the Malicious Code Protection (SI-3) control. Many organizations will run additional antivirus software on endpoints, but this feature will offer defense in depth.

### Intrusion Prevention System Features

IPS features of the FortiGate appliance can also support detection and blocking of malicious code on the wire. FortiGate not only supports the use of vendor-created and -distributed rules, but also allows end users to define their own signatures to support detection of specific malicious code.

## Supply Chain Risk Management (SR)

The Supply Chain Risk Management control family of NIST 800-53v5 is concerned with evaluating and mitigating threats to the hardware and software supply chain, such as the issues that led to NotPetya and the Sunburst malware exploits. Supply chain risks can be both direct and indirect. Organizations must concern themselves with the integrity of the supply chain from the manufacturer to their deployment to ensure that hardware and software are not tampered with in transit. But organizations must also address the risks posed by manufacturers supplying services, hardware, and software that are themselves compromised and shipping a compromised product. Fortinet has a robust supply chain security management system to prevent exactly this type of issue. The FortiGate appliance contributes to some controls in this family but only for FortiGate itself. Deployment of a FortiGate appliance will not meaningfully contribute to compliance with the NIST 800-53v5 Supply Chain Risk Management control family for other software or hardware deployed in the network.

# Conclusion

The FortiGate appliance is a feature-rich unified threat management tool that supports features for intrusion prevention, VPN, and firewall. The features included in FortiGate make it a great choice for compliance with multiple NIST 800-53v5 controls and control families. Where FortiGate doesn't provide complete compliance with a control, it often supports partial compliance. Organizations that need compliance with NIST 800-53v5 and need to replace existing firewall, IDS, or VPN systems should strongly consider FortiGate as a candidate for deployment.

## About the Author

**Jake Williams** is a SANS analyst, senior SANS instructor, course author, and designer of several NetWars challenges for use in SANS's popular, "gamified" information security training suite. Jake spent more than a decade in information security roles at several government agencies, developing specialties in offensive forensics, malware development, and digital counterespionage. Jake is the founder of Rendition InfoSec, which provides penetration testing, digital forensics and incident response, expertise in cloud data exfiltration, and the tools and guidance to secure client data against sophisticated, persistent attacks on-premises and in the cloud.

## Sponsor

**SANS would like to thank this paper's sponsor:**