Architecting for Compliance: A Case Study in Mapping Controls to Security Frameworks

Jake Williams

A SANS Product Review

Architecting for Compliance: A Case Study in Mapping Controls to Security Frameworks

(Companion Piece to "Achieving NIST 800-53v5 Compliance with FortiGate: An Implementation Guide")

Written by **Jake Williams**

February 2021

Sponsored by:

Fortinet

SANS performed a review of Fortinet's FortiGate product to test and highlight features. SANS identified how the FortiGate product features align with NIST 800-53v5 controls. Because the FortiGate product is extremely broad in its capabilities, SANS focused on the features that are most applicable to NIST 800-53v5 compliance.

This paper is intended to assist those considering the FortiGate product family—as well as those who may be unfamiliar with FortiGate—to understand its capabilities and how it will help them achieve their NIST 800-53v5 compliance goals.

Testing Scope

Because NIST 800-53v5 is so vast, this paper highlights control families rather than individual controls. This product test report focuses on the specific product features and configuration options that contribute to addressing NIST 800-53v5 control families. Where clarification is needed to determine how FortiGate can address a control family, a note will be provided highlighting how the control family applies. For reference, the 800-53v5 specification has the following control families:

- Access Control
- Assessment, Authorization, and Monitoring
- Audit and Accountability
- Awareness and Training
- Configuration Management

- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- PII Processing and Transparency
- Planning
- Program Management
- Risk Assessment
- Supply Chain Risk Management
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition

Nearly every FortiGate feature we inspected could create logs detailing the use of the feature. This feature was a welcome change from many products that display a status on the GUI but fail to create a log of an event. Although logs are obviously a feature critical to the Audit and Accountability NIST 800-53v5 control family, we don't include it in every feature review unless the logging is part of the feature under discussion.

The remainder of this paper will address FortiGate's features and how they can be used to ensure compliance with NIST 800-53v5 control families.

Logging In

We accessed the FortiGate device through a web browser using HTTPS. Any security professional logging into a device using a web browser wonders, "Will this actually support the features I need via the web interface, or will I need to use the command line or install a proprietary management application?" In the case of FortiGate, it was immediately clear from the number of menu options that the web interface (shown in Figure 1 on the next page) would support most, if not all, required configuration directives.

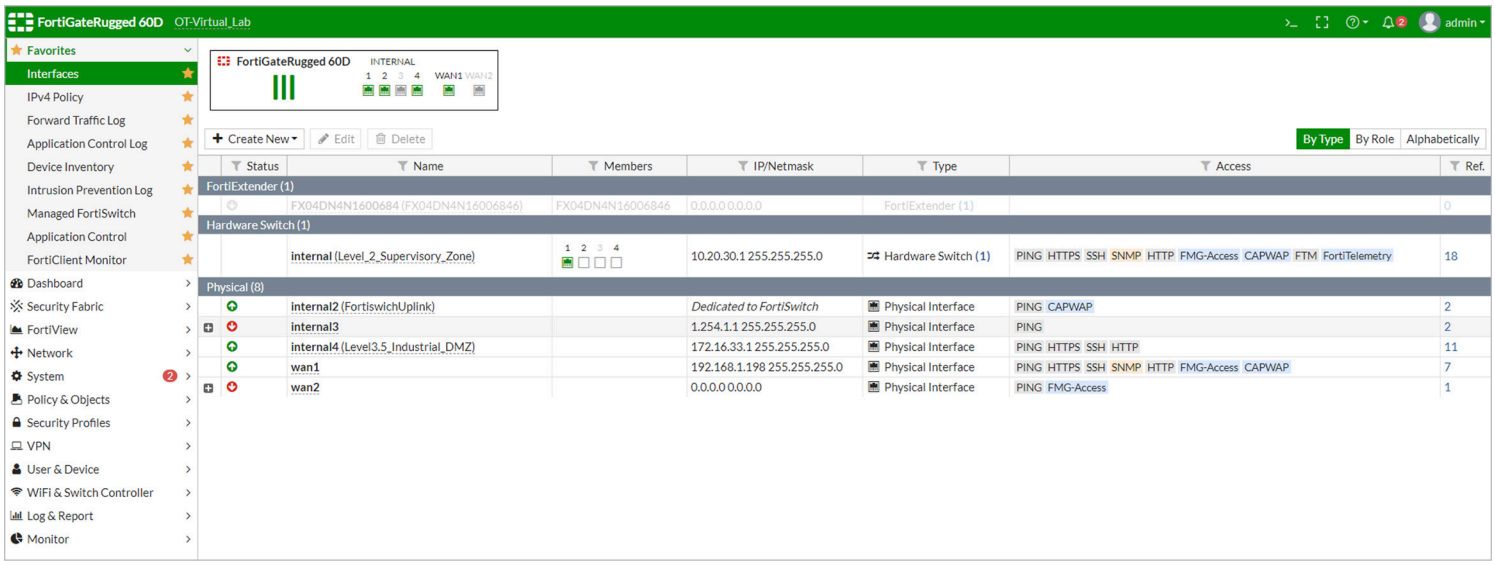

Figure 1. FortiGate Login Panel

The web interface is well thought out. Of particular benefit are the Favorites, allowing administrators to immediately jump to the specific areas of the configuration they use most. Configuring Favorites is as easy as clicking on the star to the right of any menu item, as shown in Figure 2. The order of Favorites can also be changed through drag and drop.

Figure 2. Configure Favorites by clicking the star.

If, for some reason, the administrator does need to access the command-line interface (CLI), that action can be performed directly through the web interface at the click of a button (see Figure 3). This feature prevents the need to expose additional ports (SSH, for instance) to provide in-depth configuration or troubleshooting.

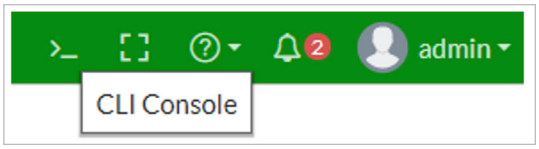

Figure 3. Accessing the CLI

These features will speed configuration tasks for the lifetime of the product. The interface has obviously been designed by actual practitioners, rather than user interface (UI) specialists.

The ability to access the CLI over HTTPS (versus the traditional use of SSH for the CLI) aligns with the NIST 800-53v5 Contingency Planning control family, specifically Alternate Communication Protocols (CP-11), "Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations."

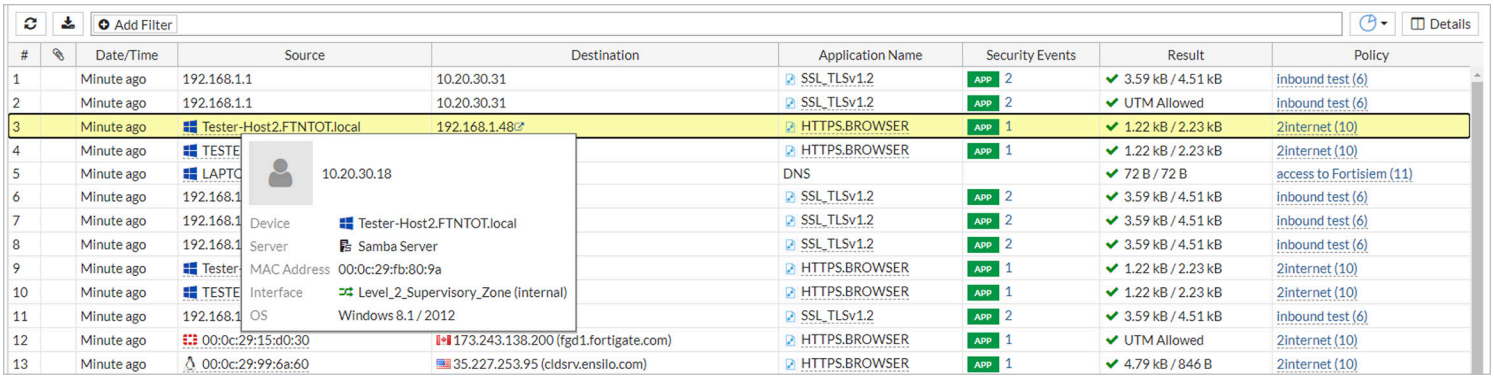

Figure 4. FortiView

Traffic Logs

The traffic log interface shown in Figure 4 is an absolute delight when compared to looking at simple NetFlow. The interface shows historical traffic seen by the FortiGate device with enough detail to quickly contextualize what is occurring. With any investigative or troubleshooting interface like this one, it is the details that matter. FortiView, FortiGate's integrated log viewing tool, provides ample details for the needs of most investigators. For instance, hovering over a hostname shows the information that is known about the device, including:

- Media access control (MAC) address
- Device name
- Service
- OS
- Source and destination byte counts
- Interface on which the traffic was seen

Hovering over the application name in the traffic log (as shown in Figure 5) shows general information about the application. Although this feature is less likely to be used by senior engineers, it is welcome among junior staff, who may not be familiar with a particular service.

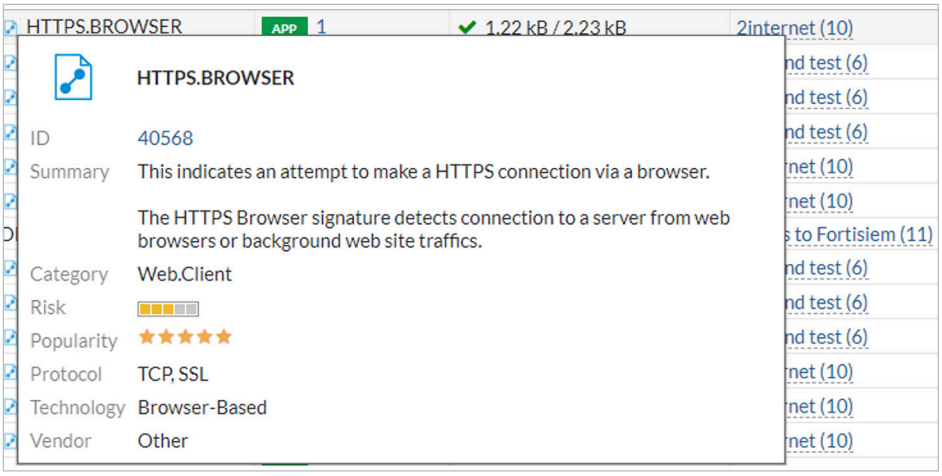

Figure 5. Application Information

Clicking on the Security Events button shows detailed information about the logged event (as shown in Figure 6). Although this information is probably logged to a SIEM in most installations, the ability to review detailed security information in the web console is extremely valuable.

As shown in Figure 7, hovering over the policy entry shows details about the policy, with clickable entries to filter on the policy and edit it as desired.

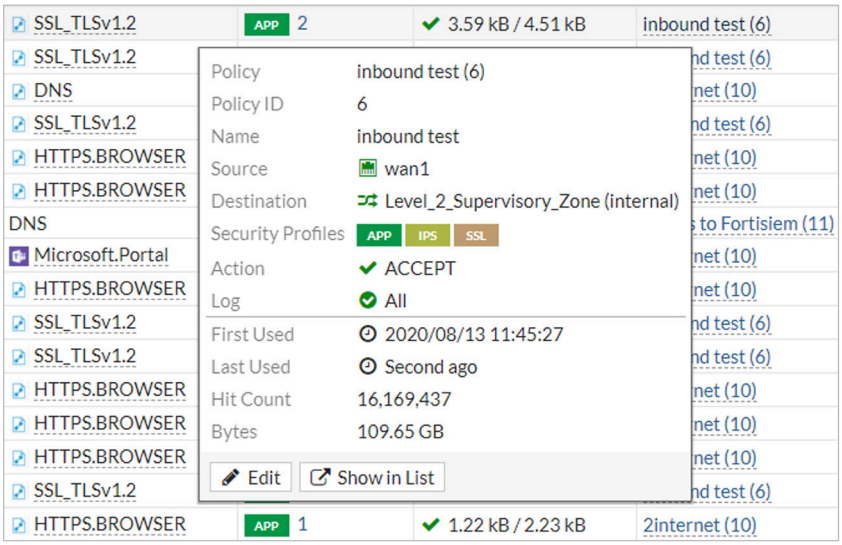

Figure 7. Policy Tooltip

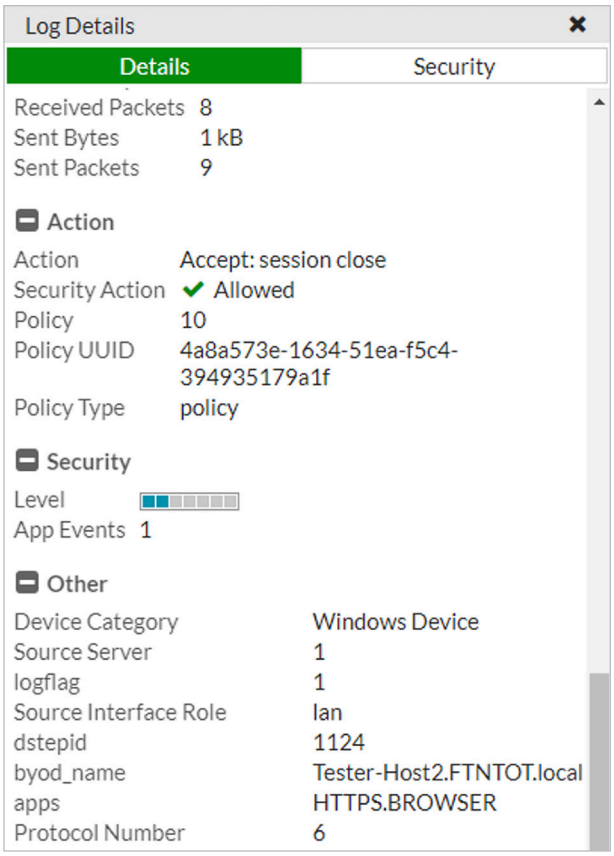

Figure 6. Event Details (Truncated Significantly for Space)

Traffic logs contribute to compliance with the following NIST 800-53v5 control families:

- **Audit and Accountability**
  - Traffic logs allow auditors to ensure compliance with policy directives.
- **Assessment, Authorization, and Monitoring**
  - Traffic logs support the requirement for continuous monitoring.
- **Configuration Management**
  - Detect devices that are improperly configured with illicit services.
- **Incident Response**
  - Identifying device communication patterns is critical during incident response.
- **Risk Assessment**
  - Review historic logs (including network traffic logs) and identify discoverable information (service information) passively.

Device Inventory

The device inventory, shown in Figure 8, displays all devices that FortiGate identifies, including information about whether the device is believed to be online or offline (based on whether traffic has been sent recently). As is standard throughout the FortiGate interface, many items allow for clickable pivots, taking you exactly where you need to go to change or view a relevant configuration item.

Status	Device	User	Address	Interfaces	OS
Fortinet device 5					
Online	00:0c:29:36:07:9c		10.20.30.2	Level_2_Supervisory_Zone (internal)	FortiOS
Online	08:5b:0e:1e:c6:84		192.168.1.1	Level_2_Supervisory_Zone (internal)	
Online	3c:ec:ef:46:d3:b9		10.20.30.210 (DHCP)	Level_2_Supervisory_Zone (internal)	FortiCam
Online	FortiOS-VM64		10.20.30.7	Level_2_Supervisory_Zone (internal)	FortiOS
Online	RuggedOTLab		10.20.30.88	Level_2_Supervisory_Zone (internal)	FortiOS/FortiSwitch / v6.0.6 build 0076
Linux PC 5					
Online	00:0c:29:c5:e7:ff		10.20.30.239	Level_2_Supervisory_Zone (internal)	Linux / 3.16.0
Offline	00:0c:29:8c:bc:89		172.16.33.50	Level3.5_Industrial_DMZ (internal4)	Linux / 3.16.0
Offline	cdtotlab		10.20.30.212	Level_2_Supervisory_Zone (internal)	
Offline	otadmin-virtual-machine		10.20.30.238	Level_2_Supervisory_Zone (internal)	Linux / 3.16.0
Offline	otadmin-virtual-machine		10.20.30.235	Level_2_Supervisory_Zone (internal)	Linux / 3.16.0
Other identified device 1					
Router/NAT device 6					
Windows device 5					
Server 22					
Unknown device 14					

Figure 8. Device Inventory

The **device inventory** contributes to the following NIST 800-53v5 control families (all of which focus on inventory to some extent):

- **Audit and Accountability**
  - Audit record generation to understand devices on the network.
- **Configuration Management**
  - Document the baseline of devices and ensure detection of new (potentially unauthorized) devices on the network.
- **Program Management**
  - Device inventory is a primary contributor to System Inventory (PM-5).
- **Supply Chain Risk Management**
  - Counterfeit hardware devices may be identified by tracking MAC addresses.

Application Control

The Application Control interface allows FortiGate administrators to selectively monitor or block traffic by application profiles (see Figure 9). These application profiles are helpfully grouped by usage. The number of applications in each group is also shown. A separate display of how many are cloud applications is especially helpful for administrators of networks that have restrictions on cloud application usage.

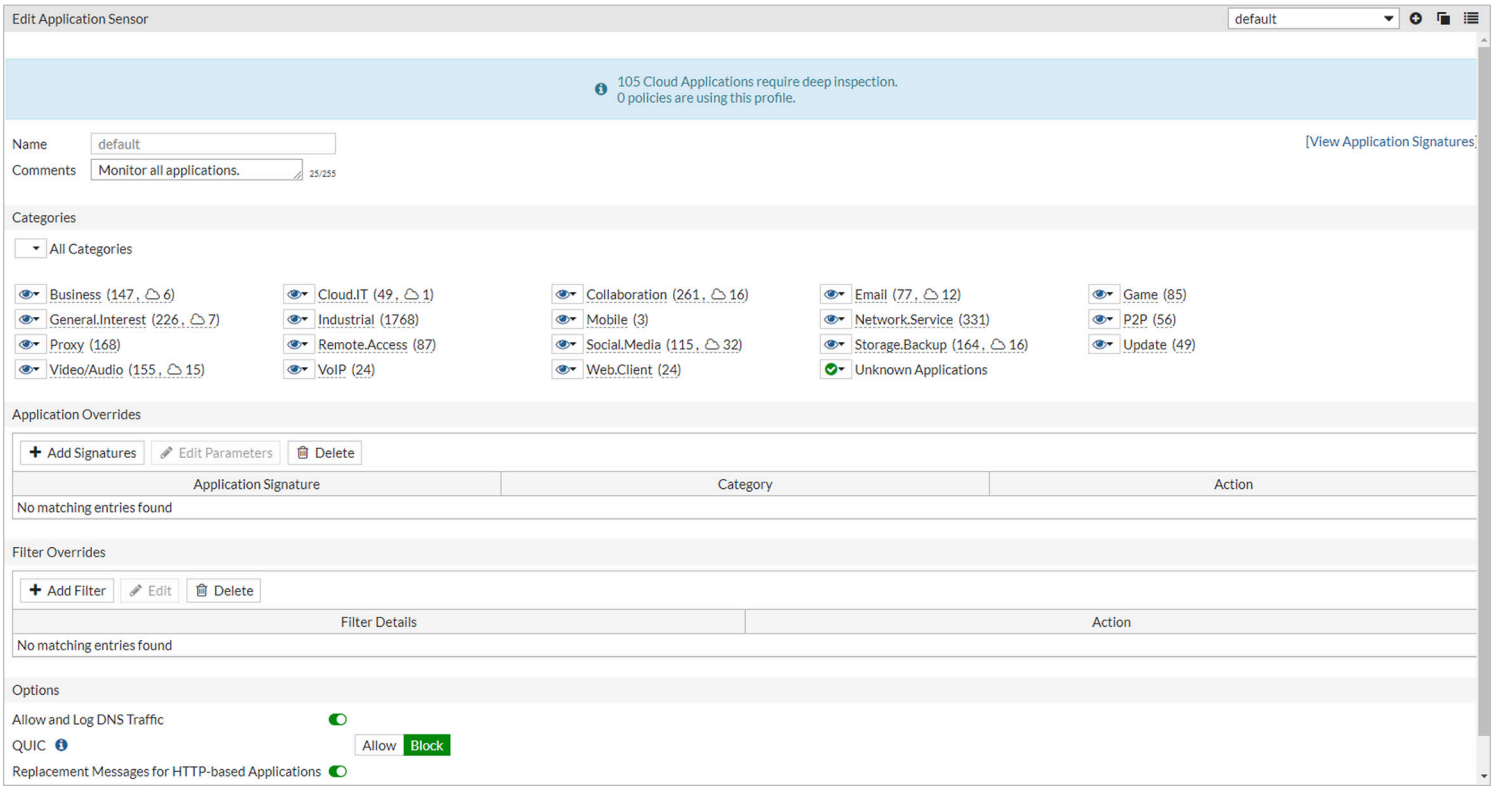

Figure 9. Application Control

The FortiGate appliance supports the blocking of Quick UDP Internet Connections (QUIC) within the Application Control interface. This forces Chrome to use TLS 1.2 and ensures that traffic can be inspected. (QUIC is not inspection-friendly.)

The logging of DNS traffic within the Application Control interface ensures that security personnel will be able to inspect logs for indicators of compromise (IOCs) when new high-profile, malicious domains are discovered. This feature is significant because many organizations still use DNS servers where the logging of requests is difficult or performance-prohibitive.

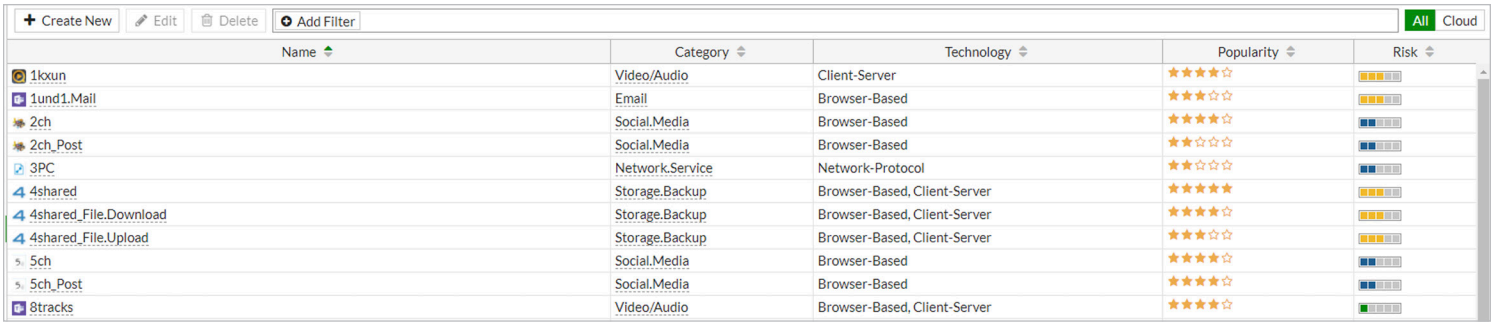

Figure 10. Application Definitions

The Application Control interface also allows administrators to deep dive into the individual applications that FortiGate knows about; it then provides a view of detailed information. Despite our testers' security tenure, we were completely unfamiliar with many of the applications defined in Application Control. It is helpful, then, that FortiGate is tracking these, because we wouldn't have been. The application definitions view (shown in Figure 10) shows individual applications that can be sorted and filtered by the following:

- Name
- Category
- Protocol
- Popularity
- Risk

In addition to the standard options of allow, block, and log, Application Control supports the option to quarantine traffic (see Figure 11). This concept seemed strange at first—after all, how does one quarantine network traffic? This option basically blocks access to the selected application type for a configurable period of time (default 5 minutes).

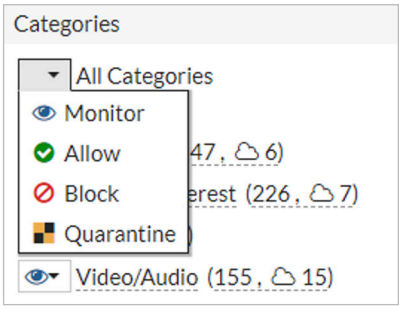

Figure 11. Quarantine Option

Application Control contributes to compliance with the following NIST 800-53v5 control families:

- **Assessment, Authorization, and Monitoring**
  - Identify when unauthorized applications are being launched.
- **Configuration Management**
  - A technical control prevents the use of applications not explicitly allowed by configuration management reviews.
- **System and Information Integrity**
  - Prevent the use of specific high-risk applications.
- **Supply Chain Risk Management**
  - A supply chain compromise may result in the distribution of software that is unexpectedly not digitally signed or has the wrong file hashes (Tamper Resistance and Detection).

Security Fabric

The Security Fabric view assists administrators in visualizing their network, both physically and logically. Figure 12 shows the logical view.

Visualization provided through the Security Fabric view is useful in understanding how devices and connections are related.

Security Fabric contributes to compliance with the following NIST 800-53v5 control families:

- **Configuration Management**
  - Visualize network configuration baselines.
- **Risk Assessment**
  - Visualization of the security fabric contributes to a proper risk assessment and risk assessment updates.

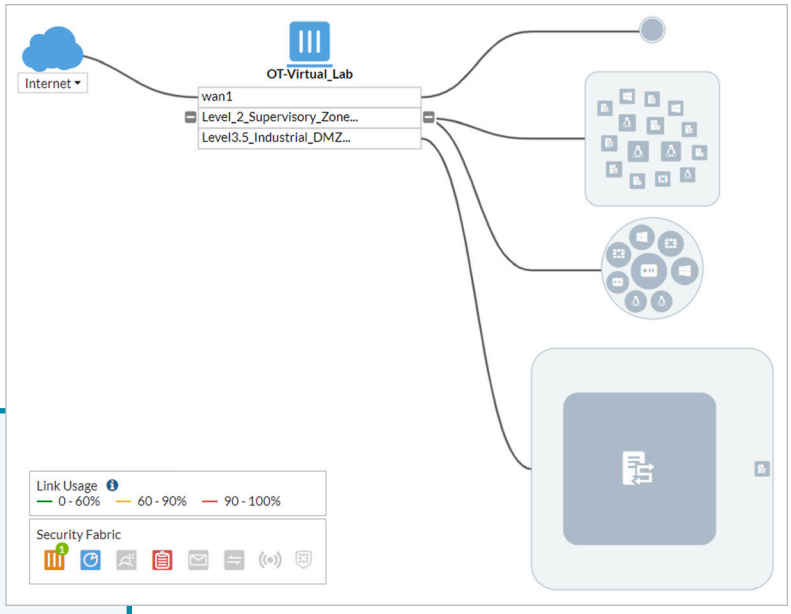

Figure 12. Security Fabric, Logical Topology

Network Firewall Rules

FortiGate supports the configuration of standard firewall rules at layers three and four and the assignment of those rules to interfaces or specific zones. The support of zones reduces administration burden by logically grouping interfaces that should share common access rules and policies. Configuring access rules doesn't require heading to the command line because FortiGate has specific access groups that can be configured in the policy editor.

FortiGate offers a robust set of options for controlling the flow of traffic between zones. A sample of the configuration options, including configuring policies by zone, is shown in Figure 13. Any network administrator who has been limited by poorly thought-out and limiting configuration options should be thrilled to see the myriad options available in the FortiGate interface. The capability to log traffic detected by the policy, whether or not it is blocked, is an excellent feature missing from many products in this class.

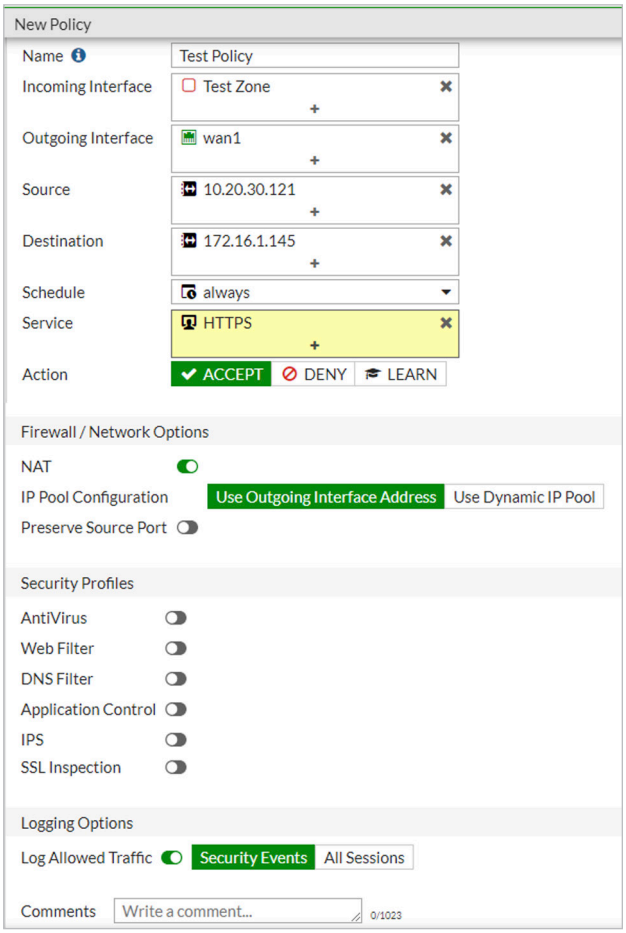

Figure 13. Policy Options

We won't spend more time in this paper examining how firewalls work—FortiGate has so many other features you won't find in a standard firewall that you'll want to devote the space to those features.

Network firewall rules contribute to compliance with the following NIST 800-53v5 control families:

- **Access Control**
  - Firewall rules limit access to resources, allowing only approved sources.
- **Audit and Accountability**
  - Firewall logs support audit functionality.
- **Assessment, Authorization, and Monitoring**
  - The firewall implements controls supporting secure information exchange.
- **Configuration Management**
  - When deployed in a zero-trust model, properly configured firewall rules prevent unauthorized configuration changes.
- **Identification and Authentication**
  - Source IP addresses can be used as a factor for authentication.
- **Incident Response**
  - Firewall rules limit the activities that must be investigated by incident response teams.
- **Program Management**
  - Firewall rules can be used as a risk management strategy.
- **Risk Assessment**
  - By understanding what actions can (and can't) be performed between network segments, firewall rules support risk assessment and risk assessment updates.
- **System and Communications Protection**
  - Firewall rules directly satisfy the Boundary Protection control.
- **System and Information Integrity**
  - Firewall rules can prevent the delivery of email from servers known to be prolific spammers, satisfying the Spam Protection control.

Intrusion Prevention System (IPS)

Intrusion prevention is a classic use case of network security appliances. However, many operations teams are reluctant to use them in all but the highest-profile attack scenarios.

Although all IPSes support vendor-managed and -distributed signatures, experienced security personnel know that they frequently need to configure custom signatures. To that end, FortiGate gives administrators the capability to configure their own custom rules. We had originally hoped the syntax for custom rules would follow the Snort convention, but we quickly discovered that the language syntax FortiGate uses is likely more user friendly, especially for junior administrators.

One of the features we really liked was the capability to effortlessly filter on specific file types with the file type directive. Another feature we really appreciated was the capability to log the MAC address of a Dynamic Host Configuration Protocol (DHCP) client. All too often during an investigation, analysts will review logs showing the IP address of a DHCP client only to discover that the DHCP logs are not available. This situation leaves the analyst with the knowledge that a security event occurred, but no idea how to investigate it. Even when DHCP logs are available, we can't imagine analysts not wanting these additional data at their fingertips.

IPS contributes to compliance with the following NIST 800-53v5 control families:

- **Access Control**
  - IPS signatures can be used to detect unauthorized access attempts and enforce access (depending on system design).
- **Configuration Management**
  - IPS can be used to identify unauthorized configuration changes by detecting traffic patterns.
- **Incident Response**
  - Information spillage can be identified and prevented by IPS signatures.
- **Risk Assessment**
  - IPSes are explicitly noted as a capability useful for the Threat Hunting control.
- **System and Communication Protection**
  - Intrusion detection and prevention are explicitly enumerated in the Security Function Isolation control description.

Wi-Fi Controller

The FortiGate appliance is capable of managing FortiAP access points and configuring profiles on each access point. Management and security features include the capability to utilize wireless intrusion detection systems (WIDS).

Wireless features contribute to compliance with the following NIST 800-53v5 control families:

- **System and Information Integrity (requires WIDS)**
- **Access Control (includes Wireless Access control)**
- **Audit and Accountability**
- **Configuration Management**
- **System and Communications Protection**

VPN Services

In our world of increased remote working, VPN services are critical. However, many organizations use VPN servers that are separate from their firewall and other security services. In many architectures, the VPN is placed behind the IPS. Although this placement ensures that attacks for which the IPS has signatures won't reach the VPN server, it creates a new blind spot for network security teams: A user connected to the VPN server may pass malicious traffic into the network without detection from the IPS when the IPS and VPN are separate. This truly is a situation in which an organization can't have its cake and eat it, too.

FortiGate's VPN options include the capability to require a client certificate on connection, which limits the efficacy of stolen or compromised user credentials, even if multifactor authentication (MFA) isn't enabled. FortiGate also supports granular VPN configuration options, allowing different users and groups to be directed to different network segments.

VPN services contribute to compliance with the following NIST 800-53v5 control families:

- **Access Control**
  - The Remote Access control specifically calls for the use of VPNs.
- **Identification and Authentication**
  - Users accessing internal resources through a VPN connection are already authenticated to the VPN service, providing additional identification information to log sources that may not already have it.
- **System and Communications Protection**
  - The Boundary Protection control specifically calls for the use of VPNs.

Antivirus

FortiGate supports antivirus definitions that can be used on endpoints and mobile devices (see Figure 14). 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.

FortiGate's antivirus scanning is already a great example of defense in depth. Although we can (and should) have antivirus running on our endpoints, having a network device also scan for known signatures provides additional protection.

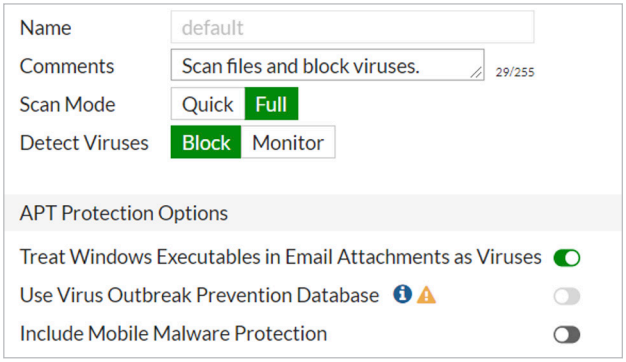

Figure 14. Antivirus Configuration

Antivirus features contribute to compliance with the following NIST 800-53v5 control families:

- **Access Control**
  - The Mobile Devices control mentions using antivirus to control unauthorized access to mobile devices, though this can be extended to other device types as well.
- **Planning**
  - Organizations must use defense in depth such that adversaries must overcome multiple safeguards to achieve their objective (Security and Privacy Architecture control).
- **System and Communications Protection**
  - Heterogeneity is supported by using antivirus from multiple vendors.
- **System and Information Integrity**
  - Antivirus clearly applies to the Malicious Code Protection control.

Web Filter

The web filter provided by FortiGate is extremely easy to configure. First, it allows for the blocking of content by generally understood movie rating levels (G, PG-13, and R). For those who need more granular control, FortiGate has them covered with specific categories and subcategories, as shown in Figure 15.

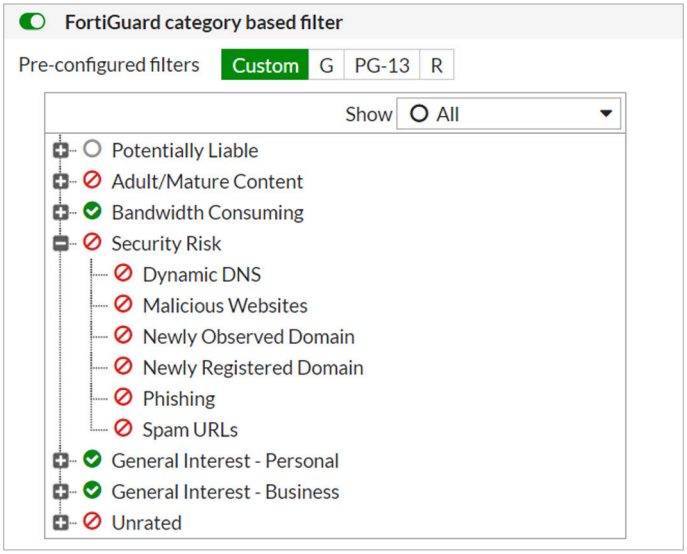

Figure 15. Filter Categories

We could write a whole paper highlighting the reasons why different categories exist and how they are useful for security administrators. Although we can't devote that sort of space here, two subcategories in the Security Risk category are especially important for catching relatively stealthy attacks:

- Newly Registered Domain
- Newly Observed Domain

The Newly Registered Domain subcategory is designed to identify when communication is attempted to a domain that has been very recently registered. Academic research has shown (and real-world experience confirms) that newly registered domains are more likely to be used maliciously than those that are a bit older. Unfortunately, it is impractical to ask users to research the age of a domain before clicking a link. Fortunately, FortiGate automatically provides that information.

The Newly Observed Domain subcategory is designed to identify when communications occur to a domain that hasn't been seen previously. This is important because all an attacker must do to beat the Newly Registered Domain heuristic is to register the domain and wait. With the Newly Observed Domain heuristic also in play, the attacker must perform far more work, delivering legitimate traffic from the domain over time before executing an attack. Although this is certainly possible, it is much more likely to be caught by security professionals in networks where FortiGate is automatically handling the more common cases.

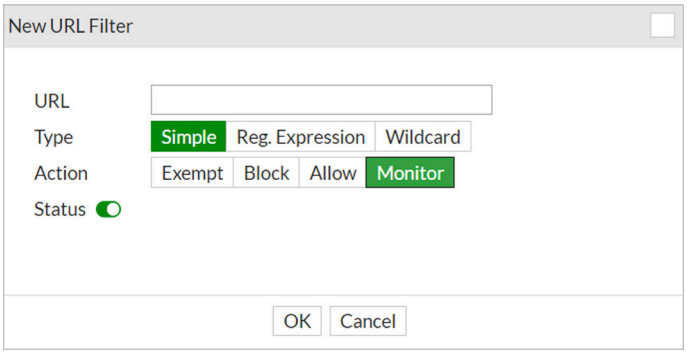

Figure 16. URL Filter

In addition to predefined domain categories, FortiGate also supports filtering based on URL filters, as shown in Figure 16. This filtering provides the capability to block or allow access to URLs, but it can also be used to create exemptions to the predefined categories. Being able to monitor access is also useful. Administrators can test a rule in Monitor mode to understand the impact of enabling it. This extremely useful feature is missing from many products, despite providing superior outcomes for security administrators.

Of course, filtering by domains and URLs doesn't always tell the whole story. Objectionable or malicious content can appear on an otherwise normal-looking domain, which often happens when attackers take over a legitimate domain (perhaps through a website vulnerability) and use it to host malicious or objectionable content. FortiGate allows security administrators to block access based on specific content in a website or page. Figure 17 shows detail on this capability. Those who work internationally will be pleased to see that many foreign character sets are directly supported by FortiGate's filtering technology.

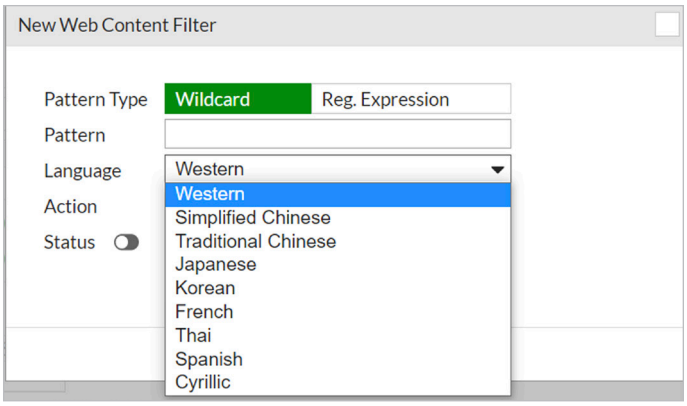

Figure 17. Web Content Filter

Web Filter features contribute to compliance with the following NIST 800-53v5 control families:

- **Incident Response**
  - URL filter logs are an excellent tool for identifying command and control traffic during incident response (IR) investigations.
- **Risk Assessment**
  - URL filtering logs are a critical source of threat hunting data.
- **System and Communications Protection**
  - URLs can be used for covert channels, such as DNS tunneling.
- **System and Information Integrity**
  - URL filtering can be used to identify malicious code that slips through signature-based detection, satisfying the Malicious Code Protection control.

DNS Filter

DNS filtering works much like web filtering, except that with DNS filtering, the site is never resolved. DNS filtering is also extremely effective in blocking access from services that are not HTTP/HTTPS-based. FortiGate supports category- and subcategory-based filtering in much the same way that web filtering works. Figure 18 provides an example.

FortiGate also supports the redirection of botnet command and control (C2) traffic to a block portal. Because botnet operators are constantly changing the location of their C2 servers, this feature requires an active subscription to be effective; however, this is the sort of service marketed by other vendors as a "DNS firewall." The fact that FortiGate includes this service as part of its core offering is extremely attractive, particularly for organizations that need to check many capability boxes with a single deployment.

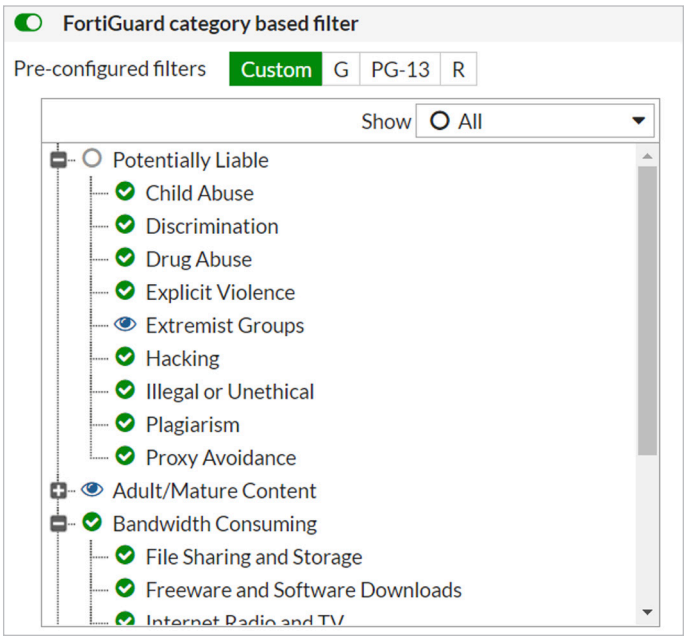

Figure 18. DNS Filtering Categories

FortiGate's DNS filtering also supports the enforcement of "Safe Search" on Google, Bing, and YouTube. Although you can't selectively enable this feature on a per-site basis (it's unclear why you'd want to anyway), FortiGate offers the option for either strict or moderate safe search enforcement on YouTube (see Figure 19).

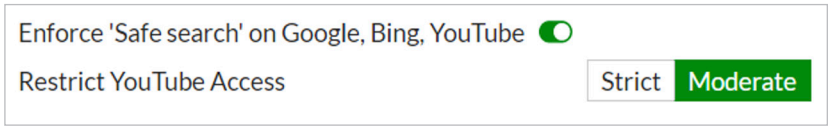

Figure 19. Safe Search Enforcement

FortiGate also supports customization of domains for its DNS filter, allowing administrators to override domains blocked by a specific category. (Figure 20 provides detail.) Blocklists for known-malicious IP addresses are also configurable. Although these are configurable elsewhere in firewall features, IP blocklists in DNS filtering work a little differently. Every DNS response returns an IP address. In many cases, attackers will have tens (or even hundreds) of malicious domains pointing to the same IP address. The external IP blocklist feature is useful in mitigating these threats.

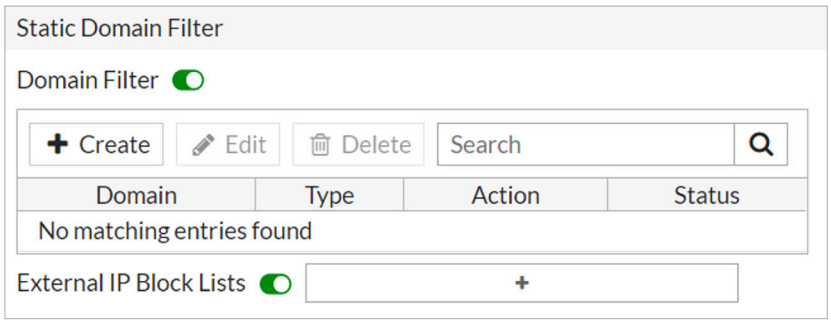

Figure 20. Static Domain Filter

As shown in Figure 21, custom domain filters provide three options to the block portal: monitor, allow, or redirect. When redirecting to the block portal, FortiGate intercepts the DNS request and provides its own response (the IP address of the block portal). Without this feature, blocking a DNS request would result in a browser or application error, likely leading to an increase in tech support calls from a user. With the redirection feature, users are taken to a site (the block portal) showing that the request has been blocked, significantly enhancing the user experience. FortiGate also allows the organization to customize its own portal, allowing the inclusion of point of contact information and links to acceptable use policies.

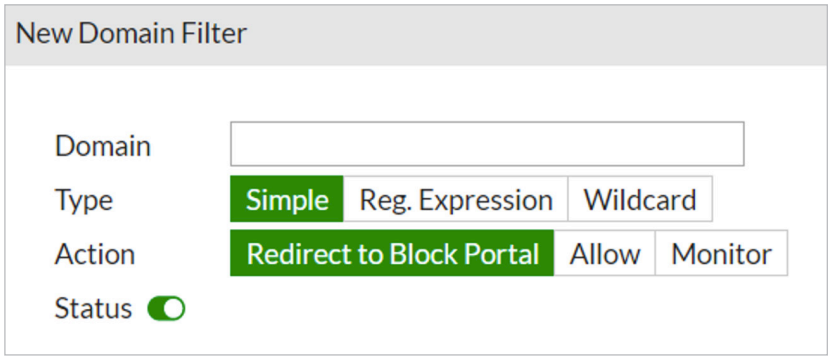

Figure 21. New Domain Filter

Lastly, FortiGate natively supports logging all DNS requests and responses. This feature is critical in all manner of investigations but particularly for security incidents. It is also 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.

The value of DNS logging was highlighted by the SolarWinds supply chain compromise discovered in December 2020.[1] In this compromise, attackers compromised the update process for SolarWinds Orion and installed a digitally signed update. Even very early after the notification, the initial domain contacted for C2 was known. Every organization that had SolarWinds Orion installed was obviously wondering, "Were we compromised?" Being able to quickly search through historical DNS logs was paramount for these organizations, many of whom were able to quickly conclude their systems never beaconed to the initial C2 domain.

[1] "Microsoft, FireEye Confirm SolarWinds Supply Chain Attack," www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack

Another valuable use for DNS logging is when only IP addresses are shared as IOCs (rather than domains). By logging DNS responses, FortiGate customers can quickly examine logs to determine if any DNS responses resolved to an IP address they have learned is malicious. Although FortiView can show connections to IP address destinations as well, the volume of the logging means that most organizations typically would have less retention on FortiView logs (30–60 days) than DNS logs (6–12+ months), allowing for a significantly different scope of investigation.

DNS Filtering features contribute to compliance with the following NIST 800-53v5 control families:

- **Incident Response**
  - DNS logs are an excellent tool for identifying command and control traffic during IR investigations.
- **Risk Assessment**
  - DNS logs are a critical source of threat hunting data.
- **System and Communications Protection**
  - DNS logs can be used to discover DNS tunneling covert channels.
- **System and Information Integrity**
  - DNS logs can identify malicious code using domain generation algorithms (DGAs), satisfying the Malicious Code Protection control.

SSL/SSH Inspection

The FortiGate appliance also supports SSL and SSH inspection, a feature typically seen only in much more expensive appliances. This is another section we could write an entire paper on, touting the many security benefits and niche configurations; however, due to the scope of this paper, we'll only highlight a few use cases.

The SSL inspection configuration allows organizations to view the list of trusted certificate authorities (CAs). We would have preferred the capability to add and remove our own trusted CAs, but this is a fairly niche feature request. Offering administrators the capability to add their own trusted CAs could also be a security issue, so it's understandable why it isn't an option.

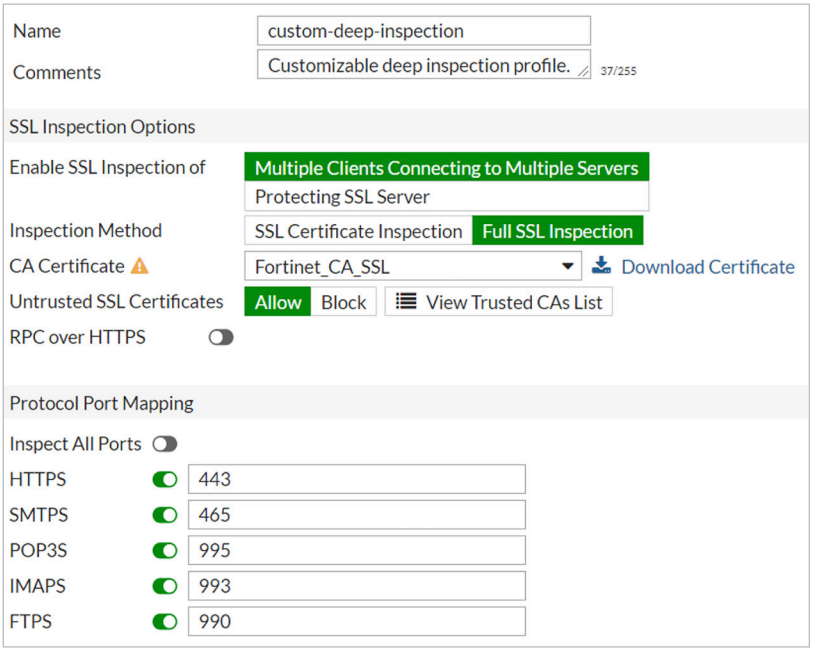

Figure 22. SSL Inspection

Administrators can, however, block all untrusted CAs (shown in Figure 22). A surprising amount of malware still uses communications underpinned by untrusted certificates, so this is an extremely useful feature that renders those samples ineffective.

Any device that allows for inspection of SSL should provide options for exempting destinations from such inspection. More data aren't always a good thing for security teams, especially when users believe they have a reasonable expectation of privacy for some operations. For instance, although employees know that their email is subject to monitoring, they likely wouldn't expect that their online banking session is subject to inspection.

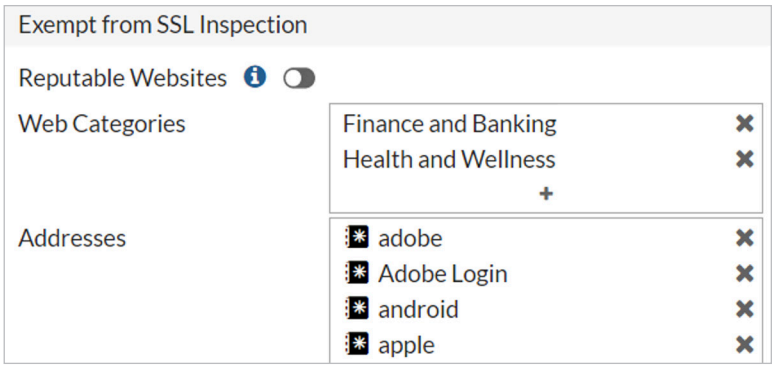

Figure 23. SSL Inspection Exemptions

As shown in Figure 23, FortiGate allows for exempting destinations from SSL inspection using multiple configuration options, including:

- Reputable websites (as identified by Fortinet)
- Categories
- Specific sites (supports domain wildcards)

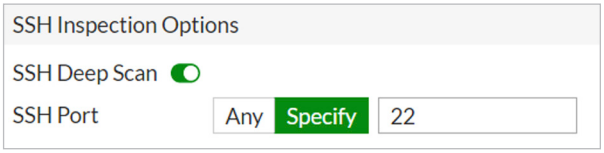

Figure 24. SSH Inspection Options

FortiGate's SSL inspection also provides the capability to monitor SSH on ports other than 22 (see Figure 24). Attackers will often change the port they use for SSH as a way to avoid inspection, but FortiGate can be configured to handle SSH on any port.

SSL Inspection features contribute to compliance with the following NIST 800-53v5 control families:

- **Configuration Management**
  - Some systems administrators use SSH tunneling to avoid the detection of unauthorized configuration changes.
- **Incident Response**
  - Encrypted communications are a black box for investigators. SSH/SSL inspection must be considered in the IR planning phase in order to avoid this issue.
- **PII Processing and Transparency**
  - Most personally identifiable information (PII) transmitted across a network is encrypted. Breaking SSL will change these dynamics for PII, and this should be included in the Policy and Procedures and Privacy Notice controls.
- **Risk Assessment**
  - Decrypting traffic a user believes to be encrypted creates additional risk for storage and inspection and should be captured in an enterprise risk assessment.
- **System and Communications Protection**
  - Encrypted traffic is normally not inspected, but understanding what is being passed is critical for network visibility and identifying the best candidates for TLS 1.3 with Perfect Forward Secrecy.
- **System and Information Integrity**
  - Without encrypted traffic inspection, malicious code may use known signatures for command and control or data exfiltration.

FortiClient Compliance Monitoring

When coupled with FortiClient on monitored endpoints, FortiGate can be used to block access to the network from hosts that have unpatched vulnerabilities. Figure 25 presents a screenshot of this function, which can ensure network hygiene while functioning as a sort of network access control (NAC).

Additionally, FortiGate can configure monitoring for FortiClient to ensure that specific applications either are or are not running on an endpoint prior to allowing communications. (A "warn only" mode is also available.) This feature can be considered a minimal implementation of allow-listing and block-listing at the endpoint. The options include validating the application by process names and SHA256 signatures. See Figure 26 for details.

Security professionals experienced with configuring application allow- and block-listing will note that the options in this configuration are limited. For instance, there is no capability to allow- or block-list dynamic link libraries (DLLs)—something very few organizations do anyway. There is also no capability to configure by digital certificate fingerprints. However, these objections dismiss the fact that the unified threat management (UTM) has any allow- or block-list features in the first place. For many organizations lacking these capabilities today, the value proposition of using a FortiGate appliance is clear because it solves multiple challenges.

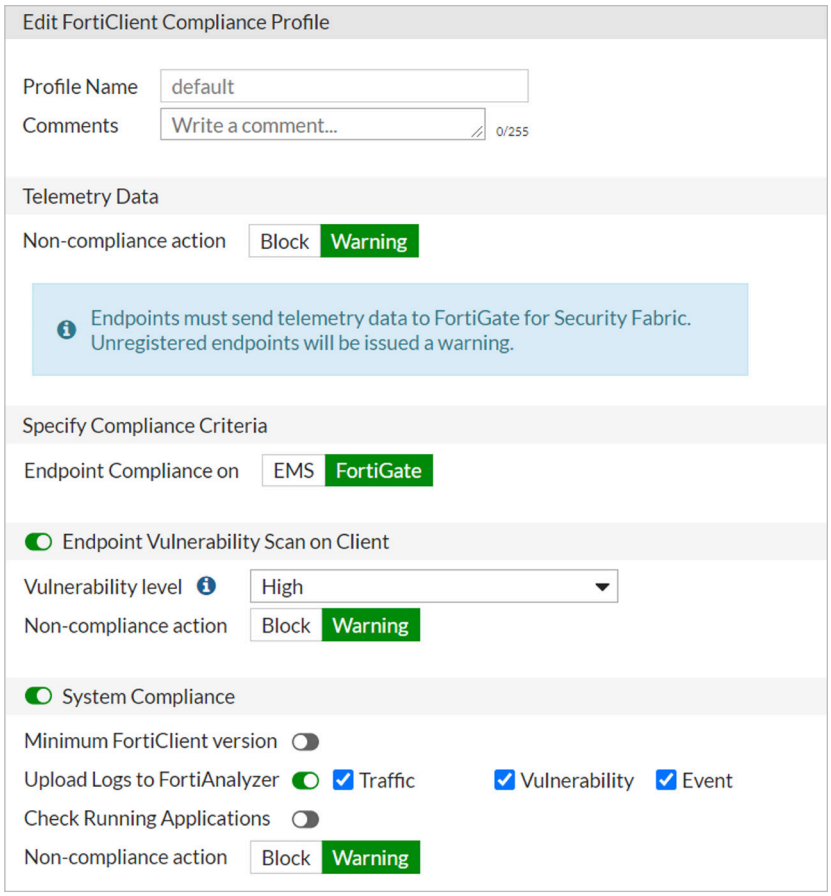

Figure 25. FortiClient Compliance Options

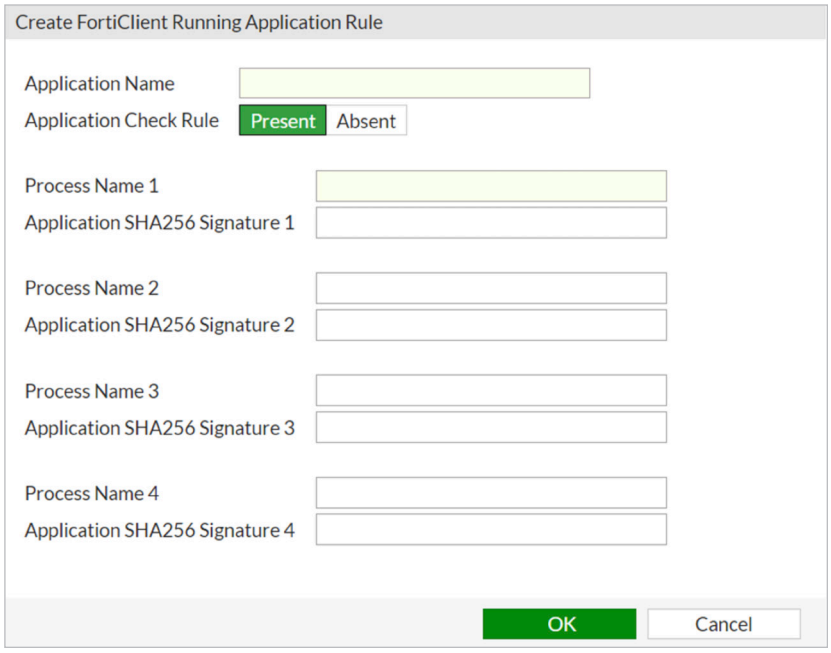

Figure 26. Application Rules

The FortiClient compliance features also include the option to ensure that various protection settings are configured on each managed endpoint (and block noncompliant endpoints from accessing the network). Options for configuration include ensuring that host-based firewalls are configured (managed by FortiClient) and that appropriate endpoint protection software is configured (see Figure 27 for detail). The FortiSandbox feature (not tested) supports directly scanning files discovered by FortiClient in a safe environment.

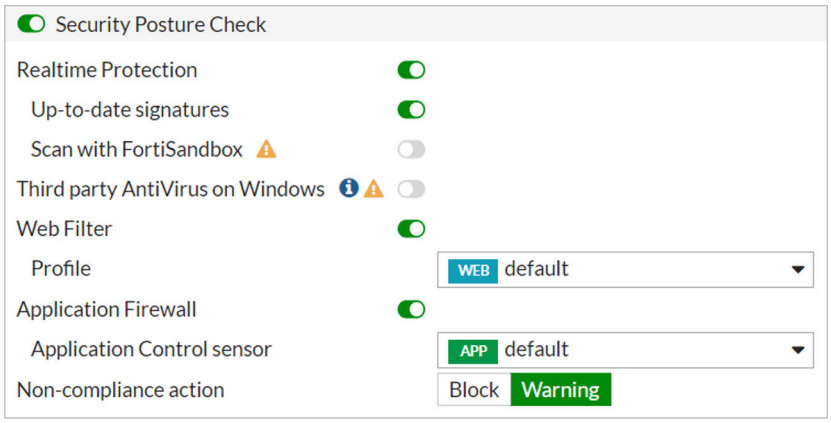

Figure 27. Security Posture Check

FortiClient Compliance Monitoring features contribute to compliance with the following NIST 800-53v5 control families:

- **Access Control**
  - Compliance monitoring creates an additional level of checks to ensure that only authorized devices can access network resources.
- **Audit and Accountability**
  - Fortinet Compliance Monitoring creates additional audit records.
- **Configuration Management**
  - Compliance monitoring is used to identify unauthorized configuration changes.
- **Identification and Authentication**
  - Compliance monitoring can be used as an additional authentication check.
- **Incident Response**
  - If Fortinet Compliance Monitoring is in place, incident responders understand the state of endpoints in the network, limiting the cost of many incident response investigations.
- **System and Communications Protection**
  - Compliance monitoring can be used to ensure that systems communicating sensitive data have appropriate controls in place.
- **System and Information Integrity**
  - Compliance monitoring directly satisfies the Malicious Code Protection control by ensuring that endpoints are running antivirus software.

User and Group Configuration

FortiGate supports all expected standards for the configuration of users and groups (particularly useful for connecting to the FortiGate VPN services), including:

- Remote Access Dial-In User Service (RADIUS)
- Terminal Access Controller Access Control Service Plus (TACACS+)
- Lightweight Directory Access Protocol (LDAP)

One nonstandard option is Fortinet Single Sign-On (FSSO). FSSO is outside the scope of this paper, but for any organization deploying FortiGate, it's something worth investigating to create a more seamless user experience. FortiGate also directly supports MFA on its appliances through the use of FortiTokens, which can be deployed as hardware or software tokens.

User and Group Configuration features contribute to compliance with the following NIST 800-53v5 control families:

- **Access Control**
  - User and group configuration can be used to ease administration of access control decisions.
- **Audit and Accountability**
  - User and group configurations create audit logs specific to identification and access to information systems resources.
- **Identification and Authentication**
  - User and group configuration directly contribute to satisfying authentication requirements.

Conclusion

The FortiGate product performed admirably in our tests and should be a contender for deployment. We found the interface easy to navigate and intuitive to operate. The features outlined in this paper form a solid foundation for complying with many aspects of NIST 800-53v5. Although no single device will help comply with all NIST 800-53v5 controls, the FortiGate product does a remarkable job of providing compliance, covering a large cross section of control families. It is all the more impressive that it does so in a way that is manageable from a single, easy-to-navigate interface. Organizations in the market for a new firewall, VPN, IPS, or UTM solution should consider deploying FortiGate to meet their specific needs.

About the Author

Jake Williams is a SANS analyst, senior SANS instructor, course author, and designer of several NetWars challenges for use in SANS' 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:

FORTINET®