Fortinet Recommended Security Best Practices

Table of Contents

Version history

April 2017: V1.0
- Initial security checks available with FortiOS 5.6.0.

February 2018: V1.2
- Renamed Security Fabric Audit to Security Rating.
- Added a new security category - SH09 Access Control and Authentication.
- Security checks available with FortiOS 6.0.0.

1 What is the Security Fabric?

The Security Fabric provides an intelligent architecture that interconnects discrete security solutions into an integrated whole to detect, monitor, block, and re-mediate attacks across the entire enterprise surface area.

2 What is the Security Rating Feature?

The Security Fabric gives a 360 degree continuous view of assets, networks and data movement within the organization. With dynamic business changes and increasing demand from on-net/off-net devices, IoT and other applications, organizations need a method to continuously monitor the effectiveness of their Security Fabric configuration.

The **Security Rating** feature provides a method to continually take a pulse of the current security posture, compare against industry peers, and assess the effectiveness in managing security risks to critical networks and enterprise assets.

3 Why would I use this Feature?

As the complex enterprise network shifts to meet evolving business needs, configurations and policies need to be dynamically changed and enforced. As a result, security measures and countermeasures need to be provisioned and tuned over in a rapid fashion which adds to the ongoing pressure on network and security teams. Inevitable errors and mis-configurations are introduced, which fail to provide the trust and assurance that critical assets are being protected.

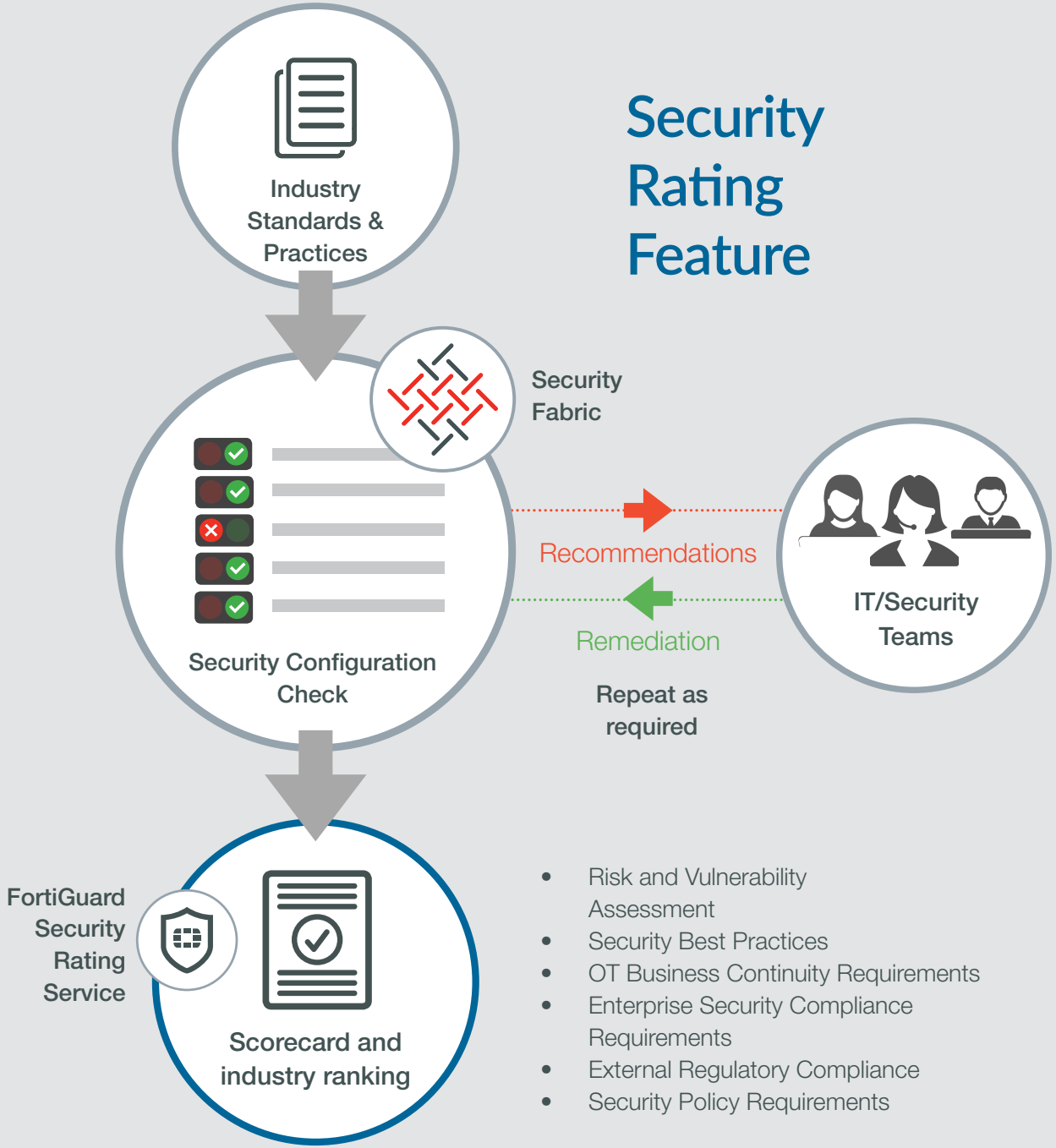
Based on **Security Best Practices and Standards**, the capabilities of the Security Fabric can be further leveraged through the **Security Rating** feature. This feature provides a mechanism to continually assess the Security Fabric, validate that configurations are working effectively, and provide awareness of risks and vulnerabilities which may impact daily business operations.

The diagram below shows the security rating reporting process flow. The Security Rating checks are performed on the Security Fabric enabled network and provide scoring and recommendations to operations teams. The Score Card can be used to gauge adherence to various internal and external organizational policy, standards and regulation requirements and ranking against industry peers through the **FortiGuard Security Rating Service**.

Key features

- Provides up to date risk and vulnerability data in the context of what is important to the business.
- Network and security teams can coordinate and prioritize fixes in a timely manner.
- As Security Fabric features and security audit checks are updated to match evolving vulnerability exploits and attacks, Security and Network teams can identify opportunities to improve systems configurations and automate processes. This results in improved network and security operations.
- Helps to keep pace with evolving compliance and regulatory standards.
- Provides a ranking against industry peers through the **FortiGuard Security Rating Service**.

Security Rating Feature



- Risk and Vulnerability Assessment
- Security Best Practices
- OT Business Continuity Requirements
- Enterprise Security Compliance Requirements
- External Regulatory Compliance
- Security Policy Requirements

3.1 Security Rating Model

The Security Rating Model depicted in **Appendix A**, illustrates how industry-standard based Security Checks can guide customers towards achieving their target security posture.

Using this integrated security controls framework, customers can tailor security checks to suit their unique security, risk and compliance goals.

Value to the Business

- Keeps customers on track with respect to their Security Roadmap and Target Security Maturity level.
- Provides Measurable and Meaningful feedback in the form of actionable Configuration Recommendations, and Key Performance/ Risk Indicators.
- Helps build Senior Management Confidence by demonstrating effective business asset protection.

Value to Additional Critical Processes

This structured approach for configuration monitoring and tuning brings value to additional critical processes.

- Supports quicker Incident Response and Remediation decisions in data breach situations.
- The status of 3rd party asset compliance can be monitored to ensure they are adhering to Enterprise Security Policies.
- Risk management teams can pro-actively monitor the status of security controls against compliance and regulatory standards.
- Brings value to Operations Teams (OT), through early awareness of potentially non-compliant assets, unstable system configuration states, and data flow anomalies.

3.2 Security Rating Feature Common Use Cases

The Security Rating Feature helps deal with complex demands common across many customers.

Use Case #1 Security Configuration Self-Assessment

Goal: NOC/SOC teams need an ongoing technical view and risk impact of configuration issues and vulnerabilities that could lead to breaches and service disruption.

How this is achieved:

1. From a **single pane**, the entire Security Fabric configuration can be assessed.
2. Identifies **configuration weaknesses** in the Security Fabric and guides best practice recommendations.

Use Case #2 Security Assurance – CISO Dashboard

Goal: CISO needs to answer the tough questions Senior Management and the Board is asking. CISO needs an overall sense of how well critical business assets are protected.

How this is achieved:

1. Highlights the **effectiveness of security investments**.
2. Provides indicator of **security posture against industry peers**.

Use Case #3 Audit and Compliance

Goal: Provide the Auditor with irrefutable evidence that the network is designed and operating according to required standards, and can allow them to confidently attest that business data is protected.

How this is achieved:

1. Integrated **Security and Compliance Framework**, based on industry-wide accepted standards.
2. **Bridges the gap** between technical configurations and audit control requirements.
3. **Customizable security checks** against specific security and regulatory standards.
4. Generate **audit-ready reports** for senior management and IT auditors.

4 Recommended Security Best Practices

These practices and standards and are intended to be a trusted source to guide customers to design, implement and continually maintain a target Security Fabric security posture suited for their organization. The Security Fabric is fundamentally built on security best practices. By running these security checks, security teams will be able to identify critical vulnerabilities and configuration weaknesses in their Security Fabric setup, and implement best practice recommendations.

The following security category checks are currently available as of the release of FortiOS 6.0.0. Additional security checks and associated recommendation will be added with future FortiOS releases.

FIRMWARE AND SUBSCRIPTIONS (FS)

Maintaining the latest software, firmware and updates on systems ensures the network is operating effectively and maintains the organization target security posture. Performing regular system configuration checks and updates allows optimal performance of the network and security devices' intended functions.

FSBP ID (FORTINET SECURITY BEST PRACTICES)	SECURITY CONTROL	TESTING PROCEDURES	GUIDANCE
FS01	**Compatible Firmware.** Ensure that the latest compatible software and firmware is installed on all members of the Security Fabric.	From the Security Fabric root, verify that all firewalls in the Security Fabric are running a version of firmware that is compatible with the Security Fabric root. From the Security Fabric root, verify that all access layer devices (Wireless & Switch) are running a version of firmware that is recommended for the firewall that they are managed by.	For any firewalls in the Security Fabric which are not running a compatible version of firmware with the Security Fabric root, upgrade them to a version of firmware that is compatible with the Security Fabric root. For any access layer devices in the Security Fabric which are not running the recommended version of firmware, upgrade them to the recommended version of firmware. Use the published Security Fabric document to validate compatible firmware versions.
FS02	**Vendor Support.** Ensure a current support contract with the vendor is in place to obtain the latest security notifications, updates and configuration management best practices.	From the Security Fabric root, verify that every firewall in the Security Fabric has a valid support contract and is registered with the vendor. From the Security Fabric root, verify that every firewall in the Security Fabric has a valid subscription to receive anti-malware and threat security check updates.	If any firewalls in the Security Fabric don't have a valid support/subscription contract or aren't registered with the vendor, then contact the vendor support center to renew/update the support and subscriptions contracts.

NETWORK DESIGN AND POLICIES (ND)

Design a business and risk driven network security architecture to ensure that only authorized business users and traffic are permitted to access network resources. Configuration design should take in account enterprise security and compliance requirements, as well as industry accepted standards for enterprise security.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	GUIDANCE
ND01	**Unauthorized access layer devices.** All access layer devices such as wireless access points and network switches should be identified and validated. Unauthorized devices should be immediately disabled.	From the Security Fabric root, verify that every access layer device detected behind a firewall in the Security Fabric is authorized to communicate with the firewall, or explicitly disabled from doing so.	Review the unauthorized access layer devices to determine if they should join the Security Fabric, and if so, authorize them from the Security Fabric root. For any unauthorized access layer devices which should not be part of the Security Fabric, explicitly disable them so that no communication takes place. Continue to log and monitor for unauthorized communication to the Security Fabric. Periodically review the logs for persistent traffic from unauthorized devices.
ND02	**Secure Wireless Connections.** Wireless networks should not permit insecure protocols such as WEP or other less secure algorithms.	***Future Release Implementation***	Unsecured wireless communications are more susceptible to attacks than physical networks. An attacker need only be in the vicinity of a location with wireless access, and can use a variety of readily available and low cost tools to ease drop on wireless communications to extract sensitive system authentication or other critical corporate information.
ND03	**Review unused policies.** All firewall policies should be reviewed every 3 months to verify the business purpose. Unused policies should be disabled and logged.	From the Security Fabric root, verify that every firewall in the Security Fabric has no configured policies which have not forwarded/blocked any traffic in the last 90 days.	Review the policies to determine if they serve a valid business purpose. If not, remove and log the policies from the firewall. Each policy and log entry should include a business and technical owner. Review all policies on a quarterly basis or monthly if frequent policies changes are required.
ND04	**Segregation of Traffic.** Separate servers from end user devices.	From the Security Fabric root, verify that every firewall in the Security Fabric has no servers detected in a segment that also contains end user devices.	End user devices should be separated from internal servers by placing them in a different segment from the server. Firewall interfaces should be labeled with a Security Profile and business purpose description. Publicly accessible servers should be placed behind an interface which is classified as "DMZ" to limit the inbound traffic to only those authorized servers.
ND05	**VLAN Change Management.** VLAN changes should be updated to all firewalls in the Fabric.	From the Security Fabric root, identify any interfaces on a Security Fabric firewall that are directly connected to 3rd party switches.	Any changes to internal VLAN configurations on 3rd party switches must be manually updated on any applicable firewalls in the security fabric. Updates can be automated by replacing the 3rd party switch with a FortiSwitch and attaching it to a suitable firewall though a dedicated switch management port. All VLAN and port assignments on that switch can be performed from within Fabric and then updated to all firewall members.

NETWORK DESIGN AND POLICIES (ND)

Design a business and risk driven network security architecture to ensure that only authorized business users and traffic are permitted to access network resources. Configuration design should take in account enterprise security and compliance requirements, as well as industry accepted standards for enterprise security.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	GUIDANCE
ND06	**Third Party Router & NAT Devices.** Third party router or NAT devices should be detected in the network.	From the Security Fabric root, identify third party router or NAT devices that are detected on any "LAN" or "DMZ" segments for every firewall in the Security Fabric.	For any 3rd party router or NAT devices that are detected, ensure they are compatible with the Security Fabric in order to provide greater visibility and control user and device traffic.
ND07	**Device Discovery.** Ensure that all systems are detected and logged on internal networks, including DMZ.	From the Security Fabric root, verify that for every firewall in the Security Fabric, any network interfaces classified as "LAN" or "DMZ" has device identification enabled, so that network topology and device movement can be monitored and reported.	For any "LAN" or "DMZ" segments which do not identify and log connected systems, update the configuration by enabling device detection on each interface of each member of the Security Fabric.
ND08	**Interface Classification.** All network interfaces should be assigned a defined and configured based on the security risk profile of the segments and systems being protected.	From the Security Fabric root, verify that for every firewall in the Security Fabric, all network interfaces are classified as either "WAN", "LAN", or "DMZ".	All interfaces should be defined according to the security profile desired for the protection of the systems placed behind them, and labeled according to the business function those systems serve. For each interface on each firewall in the fabric, assign the appropriate security profile ("WAN", "LAN" or "DMZ") and label its business function using the Alias description.
ND09	**Detect Botnet Connections.** Ensure all networks including wired and wireless access points are configured to detect Botnet activity, including any similar suspicious traffic entering and leaving the network.	From the Security Fabric root, verify that for every firewall in the Security Fabric, all network interfaces classified as "WAN" are configured to detect outgoing botnet connections.	Enable the botnet detection and blocking of those Command and Control connections on the "WAN" interface to protect the endpoint and segment from being further compromised. Enable logging and monitoring on those interfaces, and review WAN traffic logs on a regular basis to look for suspicious patterns and external IP addresses.

NETWORK DESIGN AND POLICIES (ND)

Design a business and risk driven network security architecture to ensure that only authorized business users and traffic are permitted to access network resources. Configuration design should take in account enterprise security and compliance requirements, as well as industry accepted standards for enterprise security.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	GUIDANCE
ND10	**Explicit Interface Policies.** Security policies should permit only authorized least privilege and least required traffic to/from authorized systems.	From the Security Fabric root, verify that for every firewall in the Security Fabric, all configured firewalls policies do not permit traffic to and from multiple interfaces.	Firewall policies should be as explicit as possible when defining how traffic can flow through the firewall. Any policies that are configured with multiple source or destination interfaces should be broken up into individual policies which match specific traffic to and from single interfaces only.
ND11	**Secure Remote Access.** All remote access included site-to-site and personal VPN should require at a minimum 2-Factor authentication.	***Future Release Implementation***	Remote connection initiated over untrusted networks are susceptible to ease dropping, session hijacking and other credential stealing attacks. Along with strong encryption for sessions, VPN remote users and device should use authentication means, such as tokens or digital certificates, in addition to username and password.
ND12	**Double-NAT.** Identify if the Security Fabric is performing Network Address Translation multiple times to any traffic pathway.	***Future Release Implementation***	In the use case where an Internal Segmentation Firewall (ISFW) is deployed, both the ISFW and Perimeter Firewall should consistently enforce security policies. Ensure the function, performance and security requirements of all business applications are met. Security policies depend on the data access and security classification requirements.

FABRIC SECURITY HARDENING (SH)

Vendor default configurations should be removed, including all default accounts, passwords and management settings. All unnecessary and insecure services and protocols should be disabled. Only business justified services and protocols should be permitted, logged and reviewed on a regular basis.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	GUIDANCE
SH01	**Unsecure Management Protocols.** All unsecure and non-business justified firewall management protocols should be removed.	From the Security Fabric root, verify that for every firewall in the Security Fabric, an administrator can connect and manage the firewall through encrypted protocols only.	Disable any unsecure protocols such as TELNET or HTTP that are allowed for firewall management purposes. Limit the number of Management Interfaces on each firewall. Enable only secure encrypted management protocols such as HTTPS or SSH.
SH02	**Change the Admin Account.**	The default super_admin and admin administrator accounts are well known administrator names. If this account is available it could be easier for attackers to access the FortiGate unit because they know they can log in with this name and only have to determine the password. You can improve security by changing this name to a more difficult one for an attacker to guess. Consider also only using the super_admin account for adding or changing administrators. The less this account is used, the less likely that it could be compromised. You could also store the account name and password for this account in a secure location in case for some reason the account name or password is forgotten.	The default super_admin and admin administrator accounts are well known administrator names. If this account is available it could be easier for attackers to access the FortiGate unit because they know they can log in with this name and only have to determine the password. You can improve security by changing this name to a more difficult one for an attacker to guess. Consider also only using the super_admin account for adding or changing administrators. The less this account is used, the less likely that it could be compromised. You could also store the account name and password for this account in a secure location in case for some reason the account name or password is forgotten.

FABRIC SECURITY HARDENING (SH)	Vendor default configurations should be removed, including all default accounts, passwords and management settings. All unnecessary and insecure services and protocols should be disabled. Only business justified services and protocols should be permitted, logged and reviewed on a regular basis.		
SH03	**Valid HTTPS Certificate - Administrative GUI.** The administrative GUI should not be using a default built-in certificate.	From the Security Fabric root, verify that for every firewall in the Security Fabric, the HTTPS administrative interface used to manage the firewall is not using a default (factory provided) SSL/TLS certificate.	Acquire a certificate from a trusted authority and configure the administrative HTTPS GUI interface on the firewall to use it.
SH04	**Valid HTTPS Certificate - SSL-VPN.** SSL-VPN should not be using a default built-in certificate.	From the Security Fabric root, verify that for every firewall in the Security Fabric, SSL-VPN is not using a default (factory provided) SSL/TLS certificate.	Acquire a certificate from a trusted authority and configure SSL-VPN on the firewall to use it, in place of the default certificate.
SH05	**Administrator Password Policy.** A strong password policy including upper, lower alphanumeric characters and at least eight characters in length should be in place.	From the Security Fabric root, verify that every firewall in the Security Fabric has a strong password policy in place for administrators.	Enable a strong password policy for firewall administrators. Align the policy and its management with the established corporate security policy for critical systems. This should include limiting administrator access to high trust individuals, enforcing unique username and passwords and safekeeping of backup/recovery administrator accounts.

FABRIC SECURITY HARDENING (SH)

Vendor default configurations should be removed, including all default accounts, passwords and management settings. All unnecessary and insecure services and protocols should be disabled. Only business justified services and protocols should be permitted, logged and reviewed on a regular basis.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	GUIDANCE
SH06	**Potentially Insecure Policies.** Firewall policies should permit only the least required traffic specific for the business function purposes.	***Future Release Implementation***	Maintain business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.
SH07	**Illogical Policies.** Firewall policies should permit only specific limited traffic for the business function purposes.	***Future Release Implementation***	Review firewall and router rule sets at least every six months. Restrict inbound and outbound traffic to only that which is necessary for legitimate business applications. Develop specific source and destination based firewall policies. Define valid hosts or groups as source and destinations.
SH08	**Fabric Policy Consistency.** All fabric members should be running policies that enforce consistent security measures.	***Future Release Implementation***	Create a data flow diagram illustrating the pathways of legitimate business applications across the network. Apply the appropriate security controls at each security gateway based on the access requirements and security classification of the data. A security gateway (i.e. firewall, router or proxy) bridges two or more trust zones and enforces the data access control policies.
SH09	**Access Control and Authentication.**	From the Security Fabric root, verify that for every firewall in the Security Fabric, the administrator account and all other privileged accounts are configured with least required privileges, strong authentication and account use management.	Devices should only be accessed by authorized personnel. Systems and processes must be in place to limit access on a "need-to-know" basis and according to job responsibilities. "Need-to-know" is when access rights are granted to only the least amount of data and privileges needed to perform a job. Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on policy and configuration changes are and can be traced to known and authorized users and processes.

ENDPOINT MANAGEMENT (EM)

All end user and server systems should comply with security and acceptable use policies, to ensure that users and applications activity are monitored and prevented from connecting to unauthorized and unsafe resources. Only authorized applications should be running on end user and server systems.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	GUIDANCE
EM01	**Endpoint Registration and Vulnerabilities.** The fabric should be aware of any endpoints that may be affected with malicious software.	From the Security Fabric root, for every firewall in the Security Fabric, determine if any endpoint devices are detected having critical vulnerabilities.	Endpoint protection software should be configured to protect endpoint devices and connected to a firewall for vulnerability status maintenance. All devices should be routinely scanned and resolved of any critical and high vulnerabilities immediately (1-2 days). Medium vulnerabilities should be address within 5-10 days. However other mitigation strategies, such as quarantine and network segregation, with detailed logging and monitoring, could be considered as compensating controls, if applying security patches or updates is not business feasible.
EM02	**Endpoint Compliance.** Endpoints should be verified for conformance to corporate network security and acceptable use policies. Endpoints should not be permitted to access critical network resources until compliance has been verified.	From the Security Fabric root, verify that for every firewall in the Security Fabric, any endpoint devices detected behind a "LAN" classified interface are validated against a set of security conformance specifications via ATP endpoint protection software that directly communicates with the firewall.	Install endpoint protection software on any endpoint devices, and have those endpoints register with the firewall so that they may be checked for conformance, and report any detected vulnerabilities to the firewall. Only "Compliant" end points should be permitted to access network resources.

THREAT AND VULNERABILITY MANAGEMENT (TV)

All network and user devices should be scanned for weaknesses on a regular basis to detect and prevent current and evolving malicious software threats.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	GUIDANCE
TV01	**Advanced Threat Protection (ATP).** Suspicious files should be redirected to a Sandbox environment, where it can be safely inspected and verified for malicious content.	From the Security Fabric root, verify that for every firewall in the Security Fabric, an anti-malware profile is configured to send any suspicious files to a sandbox environment for further analysis.	Enable the Security Fabric Anti-virus Security Feature, and ensure a valid Sandbox subscription is enabled. Enable the appropriate Anti-Virus profile Inspection Options based on the corporate security policy for file and executable handling.
TV02	**Endpoint Quarantine.**	***Future Release Implementation***	Malware infections and outbreaks should be identified and contained as soon as possible. A monitoring mechanism should be in place to detect malware patterns and anomalies at the host level. A compromised host should be quarantined and wiped clean of malware as soon as possible to limit wide spread contamination.
TV03	**Network Anti-Virus.**	***Future Release Implementation***	Network anomalies indicting malware traffic should be identified and prevented from further progress into critical segments.
TV04	**Host based Intrusion Prevention.**	***Future Release Implementation***	Malware infections and outbreaks should be identified and contained as soon as possible. A monitoring mechanism should be in place to detect and prevent malware patterns and anomalies at the host level. This includes the capability to detected and prevent host OS and application layer malware.
TV05	**Protection from Malicious Websites.**	***Future Release Implementation***	Access to external web sites should be filtered and logged to prevent malware from compromising end-user devices.
TV06	**Detect Malicious Applications.**	***Future Release Implementation***	Connection attempts to external web sites should be filtered and logged to prevent consuming bandwidth or other non-compliance applications from being access by end user devices.
TV07	**UTM Inspection Optimization**	***Future Release Implementation***	Changes in business requirements may require changes to security policies and traffic inspection. This may inadvertently lead to performance degradation. Enterprise application functionality and service performance requirements should not be impacted. Ensure security inspection designs and implementation settings are continuously monitored and optimized where possible.

AUDIT LOGGING AND MONITORING (AL)

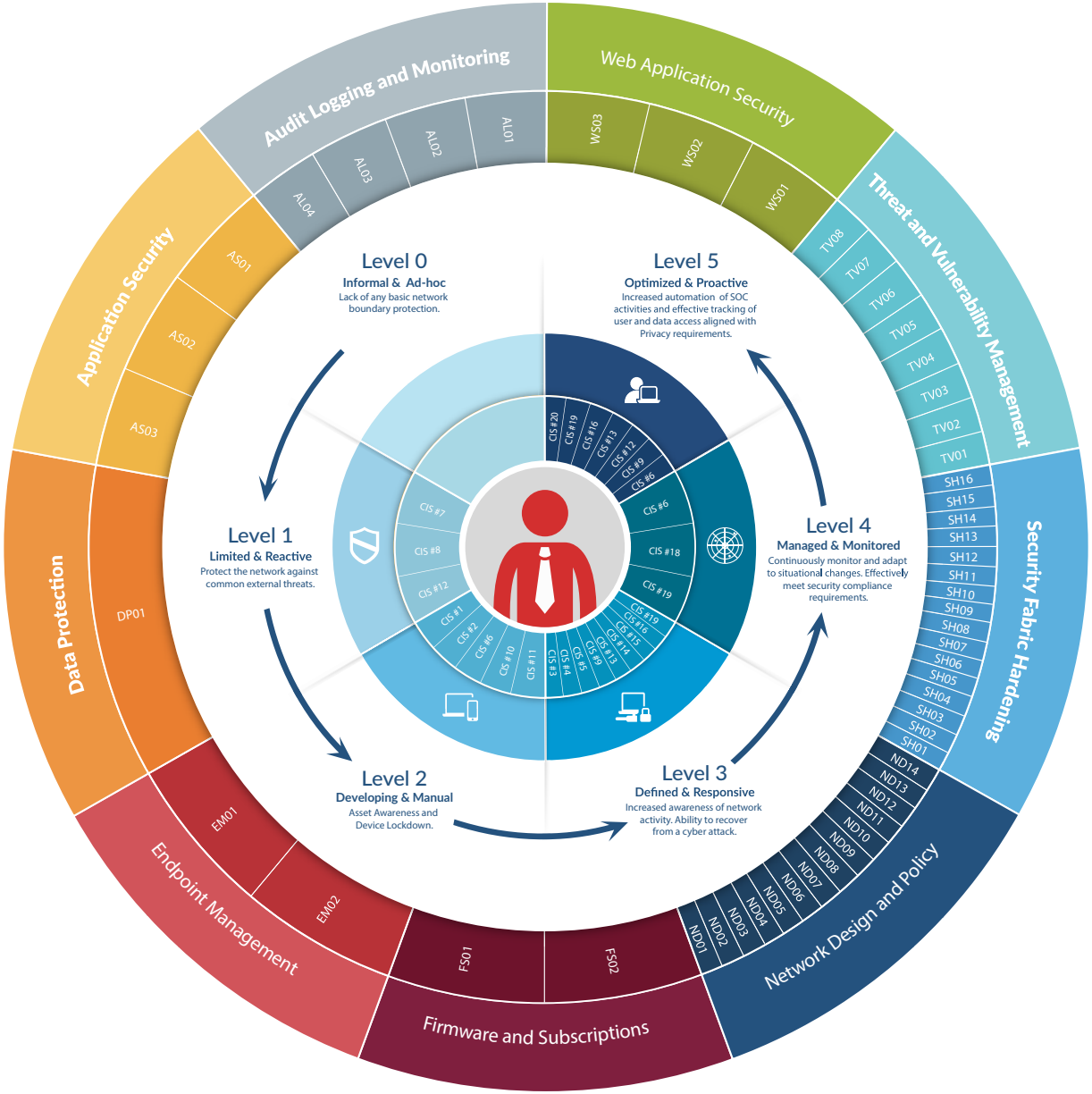
All user and traffic activity should be tracked and verified based on business priorities basis. Regulatory and other standards require specific types of logs and audit evidence to be collected over a specified period of time in order to demonstrate conformance with those requirements.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	GUIDANCE
AL01	**Look for IOC from Historical Logs.**	***Future Release Implementation***	Outbound Botnet traffic can typically hide inside of other legitimately looking business traffic, such as DNS, as it attempts to connect with external Command and Control servers. Security and traffic logs should be configured to monitor, log and alert suspicious traffic. The compromised hosts should be identified, quarantined and wiped clean of any malware.
AL02	**Centralized Logging & Reporting.** Logging and reporting should be centralized.	From the Security fabric root, verify that every firewall in the Security Fabric is sending logs to a centralized logging device within the Security Fabric.	Configure each member of the Security Fabric to send all system, traffic, and security traffic logs to a centralized location for analysis and reporting. Centralized logging and analysis reduces administrator effort in manually collecting and merging logs. Often logging servers such as FortiAnalyzer and FortiSIEM have automated and built-in capabilities to perform quicker processing and reporting based on the desired security or network analysis objective.

Appendix A: Security Rating Model

SECURITY RATING

Measurable and Meaningful Enterprise Security



SECURITY CAPABILITIES BY MATURITY LEVEL

Level 1

- Perimeter Network Defenses

Level 2

- Network devices and asset inventory.
- Acceptable software and systems.
- Harden network devices.

Level 3

- Privileged User local/remote access management.
- Physical access management.
- Access logging and monitoring.
- Backup and recovery.
- Configuration compliance checking - network.
- Compliance with internal security policies.

Level 4

- Vulnerability and threat risk scoring.
- Asset vulnerability scanning integration.
- Advanced/Active Threat Protection with external security feeds.
- Industry best practices and feature updates.
- Stronger user/client identity and access management (privileged users).
- Automated log analysis with customised application threat use cases.
- Security Awareness Reporting.
- Formal Security Operations.
- Formal Incident Response and Recovery.
- Post-Incident Analysis Reporting and Recommendations.
- Compliance Monitoring and Compliance Risk Assessment Reporting.
- Compliance with external regulatory Security requirements.

Level 5

- User behavior tracking.
- Application/data visibility and control.
- Stronger user/client identity and access management (all users).
- Data forensics analysis.
- Trend and historical Key Risk Monitoring.
- Automated threat/anomaly detection to remediation action.
- Compliance with external regulatory Privacy requirements.

CRITICAL SECURITY CONTROLS BY MATURITY LEVEL

Level 1

CIS #7 Email and Web Browser Protections.
CIS #8 Malware Defenses.
CIS #12 Boundary Defense.

Level 2

CIS #1 Inventory of Authorized and Unauthorized Devices.
CIS #2 Inventory of Authorized and Unauthorized Software.
CIS #6 Maintenance, Monitoring, and Analysis of Audit Logs – Firewall alerts.
CIS #10 Data Recovery Capability.
CIS #11 Secure Configuration for Network Devices.

Level 3

CIS #3 Secure Configurations for Hardware and Software.
CIS #4 Continuous Vulnerability Assessment and Remediation.
CIS #5 Controlled Use of Administrative Privileges.
CIS #9 Limitation and Control of Network Ports.
CIS #13 Data Protection.
CIS #14 Controlled Access Based on the Need to Know.
CIS #15 Wireless Access Control.
CIS #16 Account Monitoring and Control.
CIS #19 Incident Response and Management – Firewall/Malware software driven alerts.

Level 4

CIS #6 Maintenance, Monitoring, and Analysis of Audit Logs – System, Applications all network devices.
CIS #18 Application Software Security.
CIS #19 Incident Response and Management – Common threat and compliance use case driven. Multi-source log consolidation and normalization.

Level 5

CIS #6 Maintenance, Monitoring, and Analysis of Audit Logs – Internal threat and data ex-filtration use case driven behavior analysis.
CIS #9 Limitation and Control of Network Ports – Internal WAF.
CIS #12 Boundary Defense – Back-channel and covert channel detection.
CIS #13 Data Protection – Continuous monitoring of all clear text confidential data and PII data.
CIS #16 Account Monitoring and Control – Privileged user profiling. PII data access profiling.
CIS #19 Incident Response and Management – Integration with upstream ticket/change management systems.
CIS #20 Penetration Tests and Red Team Exercises.

*CIS Top 20 Critical Security Controls for Effective Cyber Defense.

SECURITY FABRIC CONFIGURATION CHECKS

Audit Logging & Monitoring

AL01 IOC Logs. Look for IOC from historical logs.
AL02 Centralized Logging & Reporting. Logging and reporting should be centralized.
AL03 Configure audit and logging. Audit web facing administration interfaces.
AL04 Logging Best Practices.

Application Security

AS01 Application database configuration.
AS02 Application Policy.
AS03 SSL/SSH Deep Inspection.

Data Protection

DP01 Data Loss Prevention.

Endpoint Management

EM01 Endpoint Registration and Vulnerabilities. The fabric should be aware of any endpoints that may be affected with malicious software.
EM02 Endpoint Compliance. Endpoints should be verified for conformance to corporate network security and acceptable use policies. Endpoints should not be permitted to access critical network resources until compliance has been verified.

Firmware & Subscriptions

FS01 Compatible Firmware. Ensure that the latest compatible software and firmware is installed on all members of the Security Fabric.
FS02 Maintenance Support. Ensure a current support contract with the vendor is in place to obtain the latest security notifications, updates and configuration management best practices.

Network Design & Policy

ND01 Unauthorized access layer devices. All access layer devices such as wireless access points and network switches should be identified and validated. Unauthorized devices should be immediately disabled.
ND02 Secure Wireless Connections. Wireless networks should not permit insecure protocols such as WEP or other less secure algorithms.
ND03 Review Unused Policies.
ND04 Segregation of Traffic. Separate servers from end user devices.
ND05 VLAN Change Management. VLAN changes should be updated to all firewalls in the Fabric.
ND06 Third Party Router & NAT Devices. Third party router or NAT devices should be detected in the network.
ND07 Device Discovery. Ensure that all systems are detected and logged on internal networks, including DMZ.
ND08 Interface Classification. All network interfaces should be assigned a defined and configured based on the security risk profile of the segments and systems being protected.
ND09 Detect Botnet Connections. Ensure all networks including wired and wireless access points are configured to detect Botnet activity, including any similar suspicious traffic entering and leaving the network.
ND10 Explicit Interface Policies. Security policies should permit only authorized least privilege and least required traffic to/from authorized systems.
ND11 Secure Remote Access. All remote access included site-to-site and personal VPN should require at a minimum 2-Factor authentication.
ND12 Double-NAT. Identify if the Security Fabric is performing Network Address Translation multiple times to any traffic pathway.
ND13 DDOS Protection. Layered mechanisms positioned to protect networks, systems and applications should be in place to protect against Distributed Denial of Service attacks.
ND14 Encrypt transmissions. Secure all business and operational information.

SECURITY FABRIC CONFIGURATION CHECKS CONTINUED

Fabric Security Hardening

SH01 Secure Management Protocols.
SH02 Secure the admin account.
SH03 Valid HTTPS Certificate - Administrative GUI. The administrative GUI should not be using a default built-in certificate.
SH04 Valid HTTPS Certificate - SSL-VPN. SSL-VPN should not be using a default built-in certificate.
SH05 Administrator Password Policy. A strong password policy including upper, lower alphanumeric characters and at least 8 characters in length should be in place.
SH06 Remove Insecure Policies. Firewall policies should permit only the least required traffic specific for the business function purposes.
SH07 Illogical Policies. Firewall policies should permit only specific limited traffic for the business function purposes.
SH08 Fabric Policy Consistency. All fabric members should be running policies that enforce consistent security measures
SH10 Acceptable Use Policies.
SH11 Protect critical system configurations.
SH12 Security by Default.
SH13 Disable sending Malware statistics to FortiGuard.
SH14 Change the default name of the device.
SH15 Disable auto installation via USB.
SH16 Permit only established session.

Threat & Vulnerability Management

TV01 Advanced Threat Protection (ATP). Suspicious files should be redirected to a Sandbox environment, where it can be safely inspected and verified for malicious content.
TV02 Endpoint Quarantine.
TV03 Network Anti-Virus.
TV04 Intrusion Protection for Hosts.
TV05 Protection from malicious websites.
TV06 Detect malicious applications.
TV07 Botnet protection configuration.
TV08 Network IPS.

Web Application Security

WS01 WAF Configuration Best Practices.
WS02 WAF Policy.
WS03 SSH/SSH Deep Inspection.

Visit FortGuard.com for the latest Threat Briefs, Zero-day research, PSIRT advisories and other Resources. Download the latest PDF copy of the Security Best Practices at http://fortiguard.com/security-best-practices.