Client Web Security

Architecture Guide

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

What is Client Web Security Architecture?

Web traffic is typically a Client-Server model, where the client requests a resource or asset from the server across the public internet. Most often, these web services are web pages, but web traffic can also include videos, such as those found on many social networking platforms, file sharing, and web based email. As the server hosts and provides the data, it is clear that the data, and therefore the server, must be protected from cyber-attacks.

However, with the growing threat landscape, bad actors have identified web requests initiated by clients can be attacked to gain access to business assets. For this reason, it is becoming increasingly necessary to consider client web security as well.

The focus of Client Web Security (CWS) does not mirror that of advanced threat scanning, where sophisticated signature matching identifies malicious code, rather CWS focuses on the destination and content of the traffic. This application awareness is accomplished through inspection of the traffic to understand and categorize the application's intention, and take appropriate and configurable action.

The action taken on the content of web traffic can be divided into two categories: security measures, such as preventing user credentials from being sent, and categorical filtering, such as limiting access to non-productive resources. Within these two categories, there are additional related benefits such as minimizing liability through prevention of illicit material, and reducing unrelated or non-useful web traffic, such as downloading and uploading large video files.

FortiGate is perfectly poised to leverage several NGFW components to accomplish web security. Below is a brief overview of the five components that comprise web security, and the associated FortiGate feature used to implement them.

Web security feature	Description	FortiGate Implementation
Encryption Inspection	The vast majority of web traffic, from web pages to streaming video, is encrypted. Therefore, it is critical that the FortiGate is able to see inside encrypted traffic to evaluate the information being sent and requested.	SSL/SSH Inspection Security Profile

Web security feature	Description	FortiGate Implementation
Web security and filtering	Web filtering serves as the primary shield against attacks originating from the web. The FortiGuard URL Filtering Service provides comprehensive threat protection to address threats including ransomware, credential-theft, phishing, and other web-borne attacks. It uses AI-driven behavior analysis and correlation to block unknown malicious URLs almost immediately, with near-zero false positives. The FortiGate's WAD daemon and IPS engine send the URLs to FortiGuard in real-time for category determination.	Web Filter Security Profile
DNS security and filtering	DNS category filtering can be used alongside web filtering to control user access to web resources. Additional security features are available through DNS security, such as blocking known C&C domains.	DNS Filter Security Profile
Policy enforcement	The firewall policy is the axis around which most features of the FortiGate revolve. Any traffic going through a FortiGate has to be associated with a policy. Policies control where the traffic goes, how it is processed, if it is processed, and whether or not it is allowed to pass through the FortiGate. This enables administrators to granularly apply security based on a vast combination of identifying characteristics, such as IP address, username, and certificates.	Firewall policy
Logging and reporting	Logging and reporting are useful components to help you understand what is happening on your network, and to inform you about certain network activities, such as a visit to an invalid website. Reports show the recorded activity in a more readable format. A report gathers all the log information that it needs, then presents it in a graphical format with a customizable design and automatically generated charts showing what is happening on the network.	FortiAnalyzer Logging

Using two common client web security architectures, this guide demonstrates how the above features can and should be implemented in real-world use cases. These use cases are:

- SMB and branch offices on page 5
- Education and libraries on page 6

SMB and branch offices

This architecture describes a business with assets to protect. Employees are subject to the well-defined Acceptable Use Policy that primarily is focused on protection, ensuring a secure digital workspace while also enhancing employee's productivity. To achieve this, content filtering plays a crucial role not only in safeguarding business resources but also in minimizing distractions. By restricting access to non-productive or unauthorized websites, organizations can reduce time-wasting browsing and optimize bandwidth usage, ensuring that network resources are used efficiently and securely.

Some key architecture definitions and qualifications include:

- One security appliance
  - The use of a NGFW is highly prioritized to deliver a comprehensive solution that scales and is cost effective.
- Remote workers
  - As hybrid and remote workers are becoming ubiquitous in most industries, companies are tasked with providing a Work From Home experience that mirrors that of in-office.
- Enterprise feature integration
  - FortiGate may function as a standalone security appliance, but can also integrate with a myriad of business applications and services to provide additional capabilities such as:
    - User authentication (LDAP, RADIUS, PKI, etc.)
    - Department or site-specific security profiles
    - Change control using FortiManager and enforcing policy change summary
- Logging
  - Centralized can potentially compare and contrast between branches if applicable
  - Can evaluate trends (baseline to qualify abnormal)
  - Forensics post-breach
  - Compliance requirements

It is important to note that SMB and branch architectures may find benefits from implementing content filtering too. As opposed to meeting compliance requirements for safeguarding internet access for minors, content filtering in a professional workplace is typically implemented to reduce excessive time wasting and maintain internet access equality for the employees in accordance with the company's internet acceptable use policy.

Education and libraries

Protecting users or students from web related threats is quite important, however they are often a smaller target since they don't provide access to the same level of assets that compromising a company might. This architecture is selected to highlight some advanced content filtering that may not be as relevant to businesses.

Some key features of education architecture in addition to the web security features:

- Content filtering
  - Apply content filtering based on user and user group
  - Safe search
- Additional safe guards to prevent circumvention attempts
  - Block DNS over HTTPs using external block lists
  - Inspect or block DNS over TLS

Intended audience

The target audience of this guide are technical IT professionals with an interest in understanding how and where client web security can be implemented. This may include system architects, design engineers, and IT managers who want to understand how and where web security can benefit their company. This guide targets those in the assessment and planning phase of the deployment.

About this guide

This architecture guide goes through different types of designs suitable for different types of topologies. Readers should use this to gather ideas for designing their solution.

Technology used

The following section describes the FortiGate features that correspond with the key components of client web security. This section includes the following topics:

Encryption inspection

Deep packet inspection (DPI) allows FortiGate to inspect encrypted traffic, and when configured properly, this is done transparently to the user. Certificate management, including provisioning and installing, is not included in this guide. See Deep Inspection in the FortiGate Administration Guide for more details.

Multiple clients connecting to multiple servers

In this mode, FortiGate will intercept the SSL handshake and dynamically replace the server certificate with a self-generated server certificate on the fly. This certificate will be very similar to the original server certificate but is signed by Certificate Authority (CA) that you have on FortiGate. By default, FortiGate uses an in-built, unique Fortinet_CA_SSL certificate to sign the replaced server certificate.

It is best practice to install a CA certificate on FortiGate that is signed by a trusted CA used in your organization. For SSL deep inspection it requires installing both private and public keys of CA certificate.

This mode enables the inspection of user web traffic, including encrypted DNS queries, and is the only inspection type used in this guide.

SSL exemptions

An important configuration option in deep inspection is SSL exemptions. You can use FQDN, Wildcard FQDNs, or web categories to exempt traffic from SSL deep inspection. It is important to ensure exemptions are in place to match any

requirements set forth in an employee internet use agreement. For example, many companies will not inspect traffic from sensitive categories, such as banking and healthcare.

Web security and filtering

The following features available on the FortiGate Web Filter profile provide both web security as well as content filtering. As an aspect of filtering, it is possible to implement advanced web logging to gain insight to user browsing behavior.

Component	Details	Security	Filtering
Web content filter	Blocks web pages containing words or patterns that you specify.		✓
URL filter	Uses URLs and URL patterns to block or exempt web pages from specific sources. It may leverage FortiSandbox to block malicious URLs that it discovers.	✓	✓
FortiGuard Web Filtering	Provides many additional categories you can use to filter web traffic.	✓	✓
External FortiGuard category threat feed	Use a dynamic list of URLs from an external server to apply a custom category to matching requests.		✓
Search filtering	Enforce safe search to restrict explicit websites and images from appearing in results. The filtering can be applied to YouTube and Vimeo searches as well.		✓
Credential Phishing Prevention	When credential phishing prevention is enabled, FortiGate scans for corporate credentials submitted to external websites and compares them to sensitive credentials stored in the corporate domain controller.	✓	
URL certificate blocklist	A dynamic package that is maintained and distributed by FortiGuard, used to block botnet communication that rely on SSL.	✓	
Remove Java applets, ActiveX and cookies	To enhance privacy, as well as limit exposure to aging technologies which may have significant security vulnerabilities, removing Java applets and ActiveX help reduce your attack surface. Blocking cookies enhances user privacy.	✓	
Block HTTP POST	The POST action is used by browsers to send and upload information to a web resource.	✓	

DNS security and filtering

You can apply DNS category filtering to control user access to web resources. When both a DNS and a web filter are configured on a firewall policy, the DNS filter takes precedence. DNS filter profile also provides additional security measure, both through configurable lists, as well as built-in mechanisms, regularly updated through the FortiGuard network.

Component	Details	Security	Filtering
FortiGuard Filtering	Filters the DNS request based on the FortiGuard domain rating.		✓
Botnet C&C domain blocking	Blocks the DNS request for the known botnet C&C domains.	✓	
Local domain filter	Define a local static domain filter to allow or block specific domains.	✓	✓
External IP block list	Any DNS query that passes through the FortiGate and resolves to any of the IP addresses in the external IP block list will be dropped.	✓	✓
External dynamic category domain filtering	Use a dynamic list of domains from an external server to block or monitor domains matching entries in the list.	✓	✓
Safe Search	Enable to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines		✓

Firewall policy enforcement

Firewall policies control the traffic flow going through the firewall. These instructions control where the traffic goes, how it is processed, if it is processed, and whether or not it is allowed to pass through FortiGate. There are a great number of settings that allow for policies to be very specific with the traffic that matches, allowing organizations to control and manage internet usage in accordance with their acceptable use policy and business objectives.

For Web Security, the main policy parameters are source, destination, and security profiles. Other policy components, such as source and destination interfaces, are important but are not explored in this guide.

Source

The source is the main setting that helps identify what traffic the policy should apply to. Some companies have specific subnets for specific departments that allow for policies to user source IP address to differentiate which security profiles to which departments. Others, for example, branch locations, may have one subnet for all employees. In such scenarios, user authentication also allows for the same type of granular per-department matching.

Source can be defined by:

- IP address and subnet
- Authenticated User

  - Certificate
  - SAML
  - Local
  - External authentication server (LDAP, RADIUS)
- Device identity
  - Certificate
  - ZTNA tags and security posture

Destination

When it comes to web traffic, policies often use a non-RFC-1918 addresses object as the destination. However, there are many reasons that a company may want to apply more restrictions on the destination. While it is possible to restrict access to IP addresses or ranges, within the destination field of a FortiGate policy, it is recommended where possible to use the Web and DNS Filter profiles to implement these restrictions.

Security profiles

For Web Security, there are three important security profiles:

- Web Filter
- DNS Filter
- SSL/SSH Inspection

See Web security and filtering on page 9 and DNS security and filtering on page 10.

Logging and reporting

Monitoring permitted web and DNS activity helps administrators understand a branch's web usage. Recording such as to meet external compliance requirements, internal compliance, auditing, and post-breach forensic analysis to name a few. Monitoring should be done transparently to employees and detailed in the AUP.

Some additional reasons for logging include:

- Compliance requirement
- Baseline normal behavior
- Accountability
- Forensics

FortiAnalyzer provides a centralized logging solution, available as a local appliance, can be hosted in both public and private clouds, and is offered as a service through Fortinet. In addition to being a log repository, FortiAnalyzer excels at analyzing FortiGate logs and returning them in a meaningful way. This includes reports, both pre-built and custom, alerts, as well as automation based on logs received to name a few.

Additional design considerations

Additional design considerations refer to concepts that are not the center of client web security but are still important and should be considered when evaluating different architectures.

This section includes the following topics:

Security compliance

Security compliance design considerations include the following questions:

- What accreditations for the business are required?
- How are they met? Is it PCI, NIST, or something else?

Explore some compliance requirements for various standards. They should be part of the design consideration. Compliance can also be internal, as determined by HR, legal, stakeholders, and so on.

Acceptable usage policy

The acceptable use policy (AUP) should be defined by your HR or Peoples team and provided to the IT and security team for implementation. An AUP helps protect your organization by setting standards and helping prevent misuse. The AUP also assists with fair resource allocation and sets expectations for both employee and employer. Many AUPs also address legal compliance by detailing what kind of personal identifiable information may be recorded. The key elements of an AUP include:

Element	Definition
Purpose	The intention of the policy should be clear as well as who it applies to.
Authorized use	What is permitted? Including what is expected as part of job responsibilities as

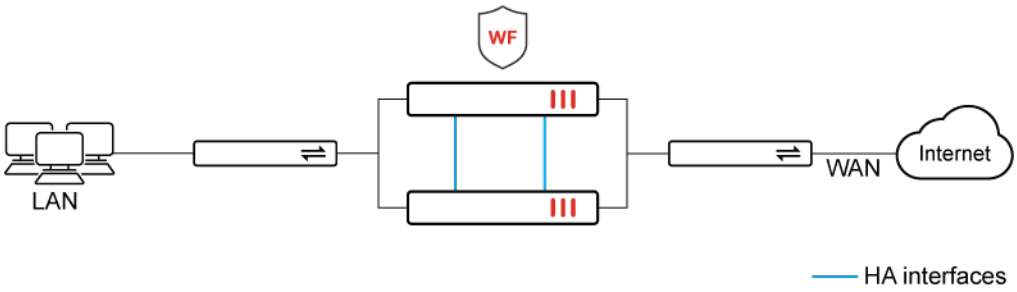
Element	Definition
	well as personal use.
Prohibited activities	Details of actions that violate the AUP, such as unauthorized access, downloading illegal content, and resource usage.
User responsibilities	Outlines the responsibilities of users. Such as password security, incident reporting, and respect of other's privacy.
Consequences	It is important to detail the results of AUP violations. The penalties should be in proportion to the violation.

Redundancy and uptime

When deploying any security measure, redundancy and resiliency should always be considered. When the FortiGate is the single point of security for a branch, in addition to being the only path to internet, you must evaluate the cost and benefit of redundancy and resiliency versus mean time to restoration in the event of a failure.

High availability

FortiGates may be deployed in High Availability to eliminate the single point of failure that is one FortiGate. There are many options for HA. See High Availability in the Administration Guide for more details.



Single points of failure should be considered across your network. For example a full mesh switching topology eliminates the single point of failure that a single switch provides by enabling data to flow through different paths and different devices. Should one device or link go down, one or more valid paths still exist. Link aggregation may also be used to address the concern of a single faulty link or interface.

Sizing

Selecting the appropriate FortiGate model (or allocating appropriate amount of resources to a FortiGate VM) will allow FortiGate to function as expected. When evaluating the various models, some metrics to keep in mind are:

Users

How many users will FortiGate be protecting? How many users are remote users that will connect via VPN? Not all users have the same traffic usage, but knowing this number can help with estimates.

Devices

This includes both company issued devices for employees, as well as BYoD and IOT devices.

Interfaces

What medium is available for the links? Do you need to aggregate some to achieve the necessary throughput? Do you have enough interfaces to support the devices you expect to connect? Foe example, this could include wireless APs, IP phones, switches, ISP equipment, and so on.

Web security throughput

Review the data sheets to learn of each FortiGate's throughput when applying client web security. This number can vary if you are doing SSL/SSH inspection (deep inspection). While web security is the focus of this guide, FortiGates are capable of providing many more security features, each with their own set of resource requirements.

Services and licensing

Service

The FortiGuard service is what keeps FortiGate up to date by providing categorization of billions of web pages, enabling users to block or allow access, with over 45 million website ratings, enhancing web filter features and providing real-time protection. When combined with DNS filtering, a vast database of known malicious and unwanted domains is used to prevent DNS-based threats and enforce internet use policies.

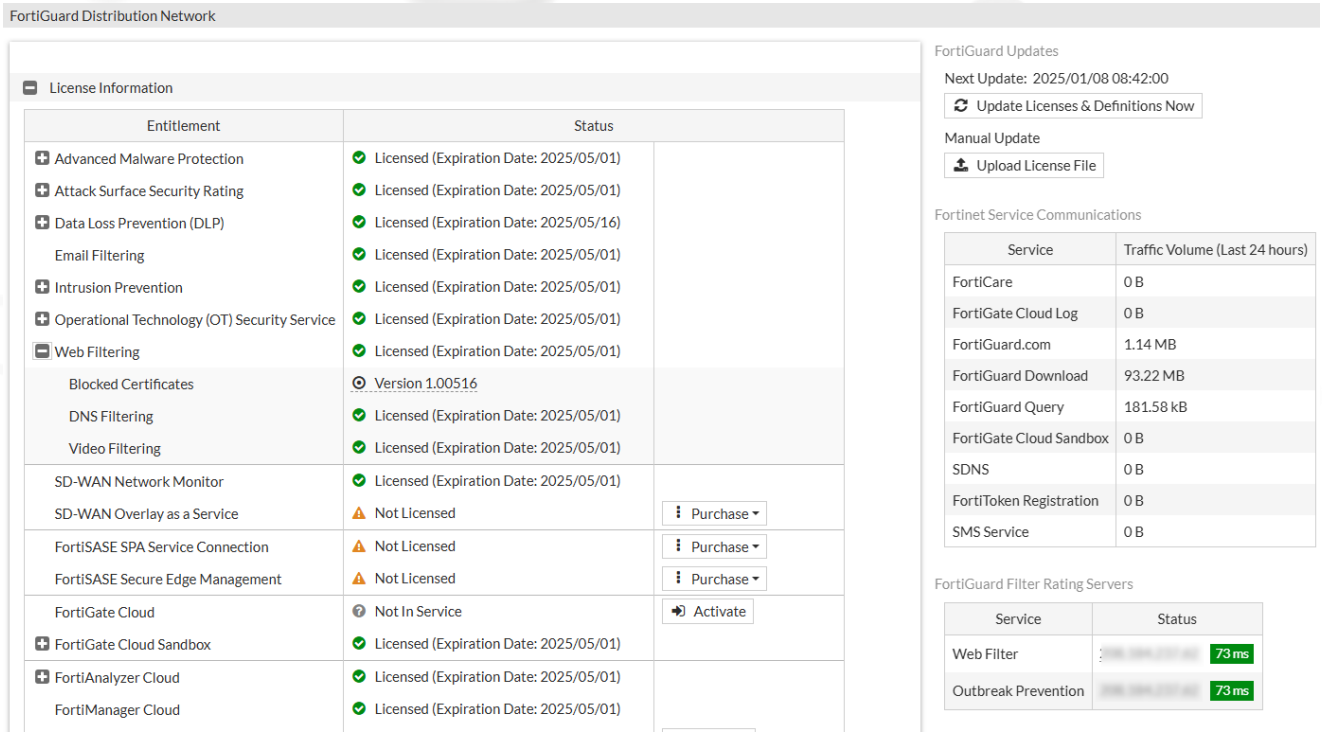
As this service is hosted by Fortinet, FortiGate requires an internet connection to receive these updates. When this is not possible in a closed network, FortiManager may be deployed as a proxy server for FortiGuard updates.

FortiManager may be implemented to provide FortiGuard updates in cases where FortiGates have internet access. See FortiGuard in the FortiManager Administration Guide for more details.

Licensing

A valid license for FortiGuard web and DNS filtering is required to utilize FortiGuard website categorization and related malicious domain lists. It can be purchased as a standalone license, and is also included in the Unified Threat Protection (UTP) and Enterprise Protection (EP) license bundles. For more details on the available licenses, see the Fortinet Security Bundles page.

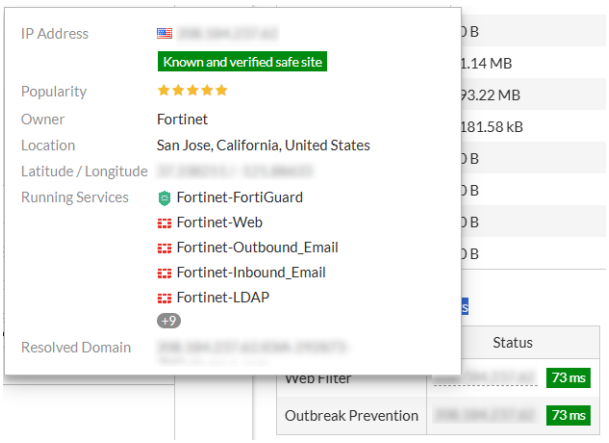
On the FortiGate, go to *System* > *FortiGuard* to find information regarding your entitlement and the status of various FortiGuard databases and engines.



Web security

On the FortiGate, go to *System > FortiGuard* and under *License Information > Web Filtering* view the information relating to web security. The list of blocked certificates version is displayed, and hovering over the version will provide the date it was updated. License status and expiration date is also displayed.

In the right side menu, the connection to FortiGuard Filter Rating Servers is shown. This details the IP address of FortiGuard servers that provides web filter service and includes response time. Hovering over the IP address displays a list of running services.



Design examples

The following architectures are explored to see where the above components can be implemented, and the effect it has:

Scenario one: Small business branch location

Requirements

In this design, a small business or branch location has unrestricted access to internet as they have limited IT personnel and are not able to deploy and manage a complex solution. Historical attempts to control and secure web traffic has fallen flat due to the lack of resources to maintain the solution as well as the disruption to employee work flow. For this reason it was removed, allowing internet access slowdowns due to streaming videos, excessive non-productive web surfing, and frequent spyware and adware infections.

With these infections becoming more frequent, the CTO has allocated budget to addressing and preventing this issue before it affects the company in a greater way, such as ransomware spreading through the entire branch and even to their limited cloud services, such as Microsoft Entra. The CTO also understands that manager and employee buy-in is important to maintain morale and productivity. For this reason it is critical that the implementation is as transparent as possible, and allow for some personal browsing.

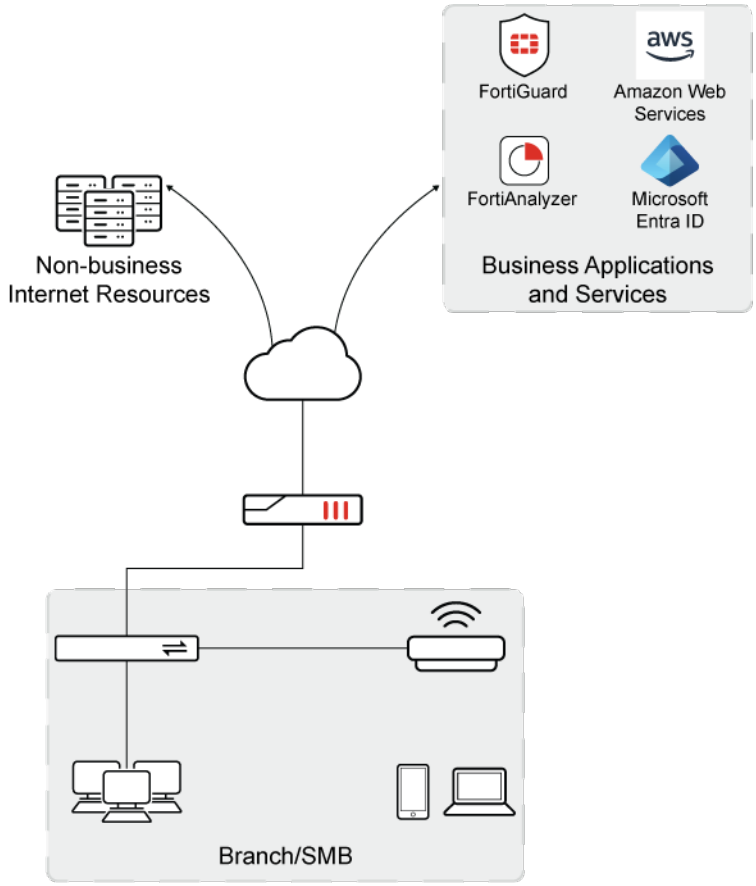
A ForitGate was selected for its low cost, ease of operation, and ability to meet the web security requirements set forth by CTO. Additionally, the ability to provide other NGFW features, such as malware protection, as a single device greatly reduces the effort required to maintain and implement this level of security.

In summary

FortiGate Feature	Required
Encryption Inspection	Yes
Web Security (WS) – content filtering	Yes

FortiGate Feature	Required
WS – Credential phishing prevention	Yes
WS – Remove Java Applets, ActiveX and cookies	Yes
SD – Block HTTP POST	Optional – Yes if business does not require uploading information.
DNS – Content Filtering	Yes
Botnet C&C domain blocking	Yes
Block DNS circumvention	Yes
Local Domain Filter	Yes, if required to allow particular domain
Firewall Policy – user authentication	Optional, if departments have differing requirements
Firewall Policy – User/department specific security profiles	Optional, if departments have differing requirements
Logging	Optional, highly recommended.

Topology



Recommendation

A small to medium sized FortiGate performs the web security and filtering for the business or branch location. FortiGate utilizes a certificate trusted by branch endpoints to enable transparent deep inspection of encrypted traffic.

A Web Filter profile is configured to filter content in accordance with the employees' acceptable web use policy that details disallowed categories. A content filter is responsible for blocking domains considered to be security threats. An additional security setting in web filter is credential phishing prevention by integrating with Microsoft Entra.

DNS filter is utilized to add additional security measures, such as blocking DNS requests that would resolve to known malicious IP addresses, and is configured to block DNS requests matching categories that are disallowed in web filter profile.

User authentication is in place and leveraged by web security to provide credential phishing prevention. This involves FortiGate connecting to corporate domain controller to check if any credentials submitted to external websites match with stored credentials.

Finally, logging is enabled and logs are sent to a central logging solution. There are many options for centralized logging, such as on-premise FortiAnalyzer, public and private cloud FortiAnalyzer, and FortiGate Cloud to name a few. Logging allows administrators to review web usage over time to assess trends and establish a baseline activity. Logging is also a requirement for many compliance standards and can assist in forensics as well.

Scenario two: Public library

Requirements

In this design, a public library is offering internet access to those with a library card. An internet and computing agreement is signed at this time. This defines what categories are blocked/disallowed, consumption, duration, etc. Access is provided through desktop PCs, and a wireless network is provided for personal devices. This wireless network may leverage user authentication or may be presented as an open and unrestricted network with a captive portal to ensure users agree to acceptable use.

Internet access is also provided for library staff, and a VPN back to the central library provides a secure connection to services such as LDAP, AD, FAZ, etc. Encryption inspection is accomplished through deploying CA Certificates on desktop PCs.

Firewall policies are configured to identify users and devices and apply web and DNS filtering profiles accordingly. For example, the kids section has PCs that are filtered in accordance with the policies set out in children's internet access section of Member Agreement.

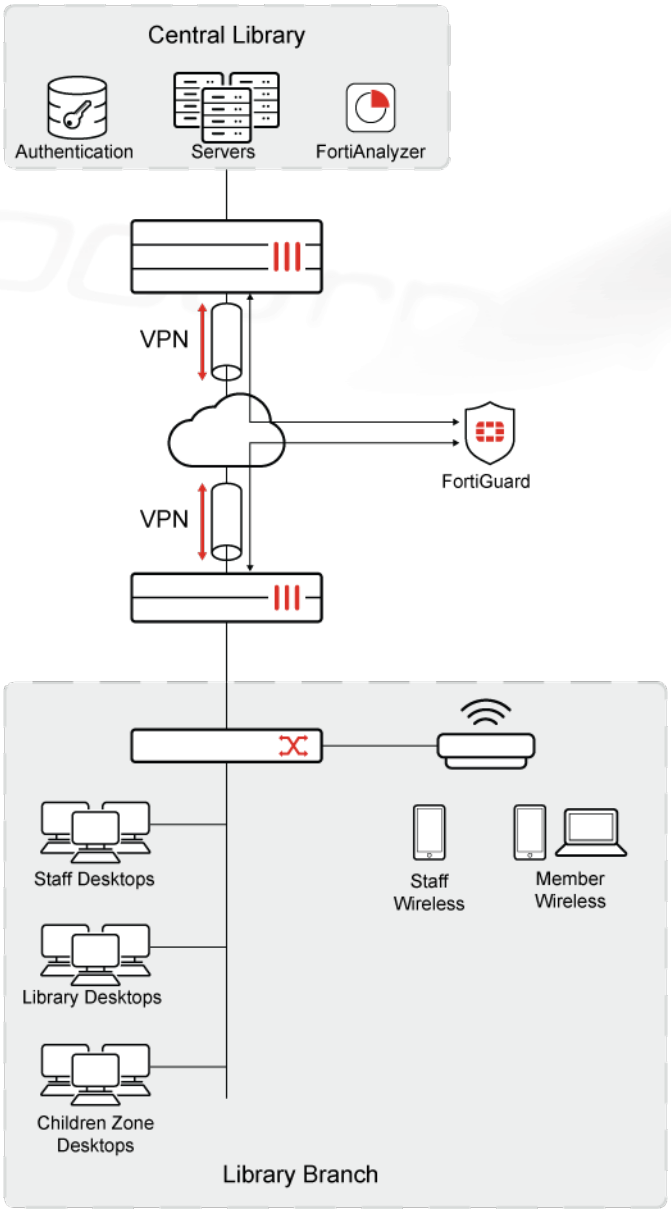
Logs are sent over the VPN back to the central library where a FortiAnalyzer stores and analyzes the data. Logs are processed anonymously and serve only the purpose of measuring resource utilization, both internet link capacity as well as AP capacity. In the event of a breach, these logs can also assist with forensics to learn how the breach happened and what actions to take to prevent it from happening again.

Branch FortiGate will also perform other NGFW features such as malware protection, IPS, etc., for library devices, and should be sized accordingly.

In summary

Feature	Staff devices	Library devices (Member desktops and children zone desktops)	Guest Wireless
Encryption Inspection	Yes	Yes	No
Web Security (WS) – content filtering	Yes	Yes	*some domain filtering
WS – Credential phishing prevention	Yes	Yes	No
WS – Remove Java Applets, ActiveX and cookies	Yes	Yes	No
DNS – Content Filtering	Yes	Yes	No
Botnet C&C domain blocking	Yes	Yes	No
Block DNS circumvention	Yes	Yes	No
Firewall Policy – user authentication	Yes	yes	Yes
Firewall Policy – User/user-group specific security profiles	Yes	Yes – Children's PCs	No
Logging	Yes	Yes	Yes

Topology



Recommendation

A medium sized FortiGate functions as the central point of security and intelligence, providing connectivity to Desktop PCs using a Fortiswitch. Additionally, wireless access points are connected to FortiSwitch and powered by FortiSwitch's PoE capability.

Web security is implemented through security profile groups to provide varying security and filtering to different user types. Library owned devices, such as staff desktops and the desktops available to members and children, are protected with the most web security features. This is possible through transparent deep inspection as the library has complete control over CA certificates used on these devices. This is in contrast to the member wireless network where no certificate management is implemented. Though the member wireless network is insecure by default, authentication to access this network is implemented using WPA2 Enterprise authentication to allow for individual authentication. This enables the library to leverage an external user identity database to dynamically enable and disable member access. Members are made aware that this network is insecure and to use at own risk.

SCENARIO TWO: PUBLIC LIBRARY

Content filtering for both the staff networks (wired and wireless) ensures unexpected and undesirable content is not available. This is for both the protection of the staff as well as library members. Content filtering for members is applied only to the member desktops and children's zone desktops. This is due to the ability to deploy and manage certificates on these devices, enabling deep inspection. The member desktops have only some categories prevented, such as sexual content and violence. Further details of permitted use is outlined in the member internet use agreement, but the decision to relax the filtering was made in an attempt to avoid restricting access to information. Children zone computers have the most restrictions in place, including safe search and only a few permitted categories.

Firewall policies are in place to control the user groups listed above. One critical aspect of firewall policies and the security profiles they contain, is their ability to log matching traffic. Logging user traffic, especially through a public service, must be done transparently to the users. Some libraries elect not to log at all to ensure user privacy is maintained. Other libraries log user traffic but apply anonymization to the logs to keep user privacy intact while gaining insight to branch use. Maintaining logs has the added benefit of facilitating forensic discovery in the event of cybercrime.

More Information

Documentation references

Feature documentation

- FortiGate Administration Guide
  - Web Filter Security Profile
  - DNS Filter Security Profile
  - SSL & SSH Inspection Security Profile
  - User & Authentication
  - Logging
- NGFW best practices – 4D Resources
- FortiGuard Web Security

Solution hub

- NGFW Solution Hub

Change log

Date	Change description
2025-02-21	Initial release.

FORTINET

www.fortinet.com

01-760-1127503-20250221