Authentication

FortiOS authentication uniquely identifies users, and based on their identity allows or denies access to security features and custom levels of UTM protection.

How FortiOS authenticates users

FortiOS authenticates users with a user name/password challenge using the HTTP, HTTPS or FTP protocol. FortiOS can also redirect HTTP authentication challenges to a secure HTTPS channel. An authentication challenge can be required whenever a user attempts a connection that is controlled by any of:

- Certificates
- Fortinet Single Sign-On (FSSO)
- Identity-based security policy
- Dynamic profiles
- IPsec VPN
- SSL VPN
- Administration access

When FortiOS receives user credentials, they are matched with a user group. If a match is found, the user is allowed access until the system-wide authentication timeout expires.

Users authenticate once to get access to multiple services. For user credential storage and access, FortiOS stores user accounts in a local user database but can also access credentials from:

- LDAP servers
- RADIUS servers
- TACACS+ servers
- FortiAuthenticator server
- Windows Active Directory servers (using NTLM)
- X.509 certificates
- public key infrastructures (PKIs)
- Two-factor authentication
- FortiToken and third party one-time password (OTP) systems

LDAP integration

Many organizations use LDAP to provide organization-wide access to information about the members of that organization. FortiOS can integrate with multiple LDAP servers and supports any LDAP server port, common name identifier, distinguished name, and one of three bind types: simple, anonymous, and regular. Communication with the LDAP server can be unencrypted or can use LDAPS or STARTTLS for secure communications. FortiAuthenticator servers can provide LDAP services to FortiOS.
RADIUS integration

RADIUS servers are used by many organizations for authentication, accounting, billing, and tracking user activities. FortiOS can integrate with multiple RADIUS servers each with its own RADIUS port, primary and secondary server IP address, and server secret. FortiOS supports PAP, CHAP, and MS CHAP v1 and v2 authentication schemes. Also supported are various RADIUS Attributes such as Microsoft Vendor-specific attributes (NAS IP/Called Station ID), the Framed-IP-Address attribute for assigning SSL VPN client IP addresses, and Acct-Input-* / Acct-Output-* attributes for accounting. FortiAuthenticator servers can provide RADIUS services to FortiOS.

TACACS+ integration

Terminal Access Controller Access-Control System Plus (TACACS+) provides similar functionality to RADIUS, but unlike RADIUS it separates authentication and authorization into two operations and uses TCP for communication where RADIUS uses UDP. FortiOS can integrate with multiple TACACS+ servers. For each server the FortiOS configuration includes the server domain name or IP address, server key, and the authentication type used by the server as one of ASCII, PAP, CHAP, or MSCHAP.

Windows Active Directory integration

FortiOS integration with Windows Active Directory provides single sign on (SSO) access for Windows users. The Fortinet Single Sign On (FSSO) agent synchronizes authenticated Windows user status with FortiOS.

Users who have already logged onto the Windows network are transparently authenticated with FortiOS identity-based security policies without a username/password challenge. FortiOS synchronizes with multiple Fortinet Single Sign On agents installed on different servers and also synchronizes with Windows Active Directory servers using LDAP. In polling mode, FortiAuthenticator can act as the Collector agent to simplify the deployment of FSSO.

NTLM integration

FortiOS also uses the Fortinet Single Sign On agent to integrate with the NTLM authentication protocol. In an NTLM configuration, when a user accesses resources that require authentication, FortiOS uses the NTLM protocol to request the logon credentials from the user's web browser and then FortiOS validates those credentials with the Windows AD server. Since this protocol uses web browsers it is essentially system independent.

The NTLM protocol protects the password by not sending it over the network. Instead, the server sends the client a random number that the client must encrypt with the hash value of the user's password. The server compares the result of the client's encryption with the result of its own encryption. The two will match only if both parties used the same password.

PKI and Certificate-based authentication

X.509 certificates provide the authentication basis for SSL-based secure communications such as SSL VPN and HTTPS. They can also provide peer authentication for IPsec VPNs. FortiOS provides a certificate database that CA and server certificates can be imported into. FortiOS also supports creating a certificate signing request (CSR) for submission to a CA, and online submission using SCEP. Certificate revocation lists (CRLs) can also be updated from online servers using HTTP, LDAP, SCEP, or local file import.

Generally certificates authenticate computers, but they can also be used to authenticate SSL VPN and IPsec VPN users. PKI user accounts can be added to FortiOS to identify the users’ certificates by a text string in the certificate (for example, an email address). The CA certificate must also be specified and be available on the FortiGate unit to verify the user’s certificate.

A special type of user group, a peer group, can be created, which contains PKI (peer) users. An IPsec VPN can be configured to allow access to any member of the specified peer group who has a valid certificate.
Two-factor authentication

To increase security, PKI users can be required to both install a certificate and to enter a user name and password. Even if an unauthorized user has access to the user’s computer, the password requirement prevents them from gaining access. Additionally, unauthorized access from a computer lacking the necessary certificate is not possible, even if the correct password is supplied. Alternately, the following methods can be used for users or administrators: a third party one-time password (OTP) system to provide a multiple digit authentication code or token, send a token via email, or send a token via SMS text messaging to a mobile device.

FortiToken

FortiTokens are an alternative to two-factor authentication with certificates, or a third party one-time password system. FortiTokens are small random key generators that provide a six digit key to accompany a username and password when logging on. When configured for a user or administrator account, the logon prompt displays the usual username and password fields and on successful entry of that information prompts with an additional field for the six-digit token or key.

Each FortiToken device’s serial number must be registered on the FortiGate unit and verified with FortiGuard servers before it can be used to logon. The FortiToken information in the FortiGate unit is always encrypted. If a token is lost or stolen, an administrator can either disable or delete it to prevent unauthorized use. A FortiAuthenticator server can easily manage large numbers of FortiTokens for FortiOS.

Identity-based security policies

Standard security policies cannot distinguish between different groups of users, and implement access levels simply according to the user’s identity. Fine-grained control of user access is possible through identity-based security policies. Identity-based security policies (IBPs) contain authentication rules that match user groups with access privileges.

When any user attempts to connect through a FortiGate unit and that connection is accepted by an identity-based security policy, the user must provide a user name and password before they are allowed access. FortiOS finds the authentication rule in the accepting identity-based policy that contains the user group where the user belongs and verifies the identity of that user. If the user successfully authenticates, FortiOS uses the information in the authentication rule to control access to firewall services (HTTP, FTP, etc.), the access schedule, the UTM protection features applied, traffic shaping, logging of accepted user sessions, and whether the user must read and accept a customizable network usage policy or disclaimer.

Dynamic Profile

Using dynamic profiles a FortiGate unit can dynamically assign different levels of UTM inspection with a UTM profile group to a user authenticated with a RADIUS server. When the user session requests access, the FortiOS unit gets the RADIUS start record for that user to confirm their credentials. FortiOS also extracts a UTM profile group name from the RADIUS start record and allows access and applies UTM features according to the security policy and UTM profile group. Dynamic profile is one way that FortiOS implements Role Based Access Control (RBAC) as user groups can be assigned different levels of network access or even limit access to a single FortiGate unit VDOM as determined by the group’s role.

IPsec VPN Authentication

FortiOS dialup IPsec VPNs accept IPsec VPN tunnel requests from any IP address and are used for remote users with dynamic or unknown IP addresses. Dialup VPNs cannot identify remote users by IP address so authentication is required to identify users.

FortiOS supports two methods to identify dialup VPN users:

- Dialup user groups: remote users add credentials to their VPN client configuration and during IPsec negotiation, FortiOS extracts the credentials and identifies and authenticates the user.
- XAuth: remote users enter a username and password to connect to the VPN. Only users who belong to the user group specified in the XAuth configuration are allowed access.

IPsec users authenticated from a RADIUS server can also have their IPsec tunnel virtual IP address assigned from their RADIUS record.
SSL VPN Authentication

FortiOS supports the creation of multiple SSL VPN portals, each providing access to a unique combination of network resources and services. Different user groups can be added to each portal and only members of the user groups added to a given portal have access to the services provided by that portal.

When an SSL VPN user logs in, their credentials are matched with a user group and the user is allowed access only to the portal that includes their user group. SSL VPN users authenticated from a RADIUS server can have their SSL VPN virtual IP address assigned by FortiOS from IP information recorded in their RADIUS record.

Authenticated user status and monitoring

FortiOS includes the user names of authenticated users in monitoring, logging, reporting, and banned user quarantine data. Log messages can be searched for user names. Reports available from FortiOS and FortiAnalyzer can identify the activities of individual users. The names of quarantined users can be viewed and their quarantine status recorded or changed.

User groups

FortiOS user groups allow organizations to provide role-based access profiles to different groups of users, for example:

- users who can access the internet at their own discretion
- users whose internet access should be filtered
- users who travel and connect to the company VPN
- users who work from home and connect to the company VPN

To support multiple access profiles, FortiOS organizes users into user groups. Administrators can then control individual user access privileges by adding users to the appropriate user groups. All FortiOS user authentication is based on adding user groups to an identity-based security policy, an SSL VPN portal, or an IPsec VPN configuration. FortiOS user groups can also be matched with RADIUS authentication server groups for advanced remote authentication, such as dynamic profiles or FSSO. If a user is part of multiple groups, FortiOS looks for the best match instead of just the first group match.

Overriding FortiGuard Web Filtering

FortiGuard Web Filtering overrides allow eligible users to temporarily disable web filtering for selected FortiGuard categories. The override can apply to the user who requested it, the entire user group to which the user belongs, or all users who share the same web filter profile. If overrides are enabled, when FortiGuard blocks a web page, the blocked user can select an override link on the block page displayed by FortiOS and enter their username and password to display the view the otherwise blocked page.

Conclusion

FortiOS’s authentication features provide the means to identify all users of FortiOS network services. Once users are identified, FortiOS can apply a wide range of individual security features to fine grained access control and traffic protection. In addition, the activities of identified users can be tracked and reported on.