How to Configure Kerberos Authentication

https://campus.barracuda.com/doc/46209142/

Kerberos works as a request-based authentication scheme and provides authentication and authorization on a single sign-on basis. The Kerberos authentication protocol provides mutual authentication, which means that both the user and the server verify each other's identity. Implementing Kerberos-based authentication within your network will allow the Barracuda NextGen Firewall F-Series to associate outgoing web requests with Active Directory users, to log user activity, and to apply user-specific or group-specific policies to outgoing connections.

In this article:

Implementation

You can use Kerberos with the Barracuda NextGen Firewall F-Series in any of the following scenarios:

- **Clients are behind a NAT-enabled router** – Requests from users on client machines behind a NAT-enabled router would appear to the Barracuda NextGen Firewall F-Series to be sent from the same reusable NAT router IP address.
- **Windows Terminal Services** – Requests from users using Windows Terminal Services to access remote data and applications on another client machine would appear to the Barracuda NextGen Firewall F-Series to be sent from the Windows terminal IP address.
- **Citrix Presentation Services** – Requests from users accessing remote data and applications on a Citrix Presentation Server would appear to the Barracuda NextGen Firewall F-Series to be sent from the Citrix Presentation Server.

Advantages

Kerberos is useful when a Microsoft domain controller is running in native mode. It is a forward proxy authentication scheme, and each authentication request against a domain controller does not need to be verified by the Barracuda NextGen Firewall F-Series.

- All users are transparently identified so that rendering DC Agents becomes unnecessary.
- All clients can use the same IP address (for example, in a terminal server environment).
- Kerberos uses a ticketing system. The user submits an initial request and afterwards has the possibility of submitting more tickets to the Kerberos ticketing system. Users do not continuously receive pop-up authentication messages when the initial authentication is

processed.
- Usage of unique Service Principal Names (SPNs) makes automatic transparent authentication possible with network resources
(each resource has its own SPN).

Requirements for Using a Kerberos Authentication Server

Before you integrate with a Kerberos authentication server, verify that the following requirements have been met:

- MSAD authentication is configured. Kerberos requires the MSAD authentication scheme.
- MS-CHAP authentication is configured.
- A forward proxy is deployed on the Barracuda NextGen Firewall F-Series. For more information, see How to Set Up and Configure the HTTP Proxy.
- The management IP address, hostname, domain, and proxy are DNS-resolvable. Check your settings on the following pages:
  - **IP Configuration** page (**CONFIGURATION > Configuration Tree > Box > Network**).
  - **DNS Settings** page (**CONFIGURATION > Configuration Tree > Box > Administrative Settings**).
- The DNS server can resolve IP addresses in both forward and reverse.
- Use type A DNS records for the Kerberos Key Distribution Center (KDC). There are known issues with some clients forming an incorrect SPN request when CNAME DNS records are used.
- Configure all host machines to use NTP. All clocks must be synchronized within 5 minutes of the Kerberos server clock for authentication to succeed.
- Time server settings must be configured on the Barracuda NextGen Firewall F-Series. For more information, see How to Configure Time Server (NTP) Settings.

Configure Kerberos

After verifying that the requirements for using a Kerberos authentication server have been met, complete the steps in the following sections to implement Kerberos on the Barracuda NextGen Firewall F-Series:

Step 1. Configure Kerberos for the HTTP Proxy Service

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. Click **Lock**.
3. In the left navigation pane, select **User Authentication**.
4. Next to **Authentication Settings**, click **Set**.
5. From the **Use Kerberos** list, enable Kerberos.

6. In the **Kerberos Service Name** field, enter a name for the Kerberos service. This name represents the IP address of the HTTP Proxy service and is used for joining the Kerberos service to MS Active Directory. The name must also be present in the **DNS Settings** section (**CONFIGURATION > Configuration Tree > Box > Administrative Settings**).
7. In the **Authentication Worker Kerberos** field, enter the number of workers started for authentication if required (default: 5).
   For proxy servers with a high load, you can enter up to 48.
8. In the **Authentication Service Settings**, select **MS Active Directory** from the **Authentication Scheme** list.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

All configured services and service names must be fully DNS-resolvable within the configured domain.

Step 2. Join the Domain

After you configure the Kerberos authentication scheme and the HTTP Proxy service, register the Barracuda NextGen Firewall F-Series and the HTTP Proxy service at the domain.

1. Go to **CONTROL > Box**.
2. In the left navigation pane, expand **Domain Control** and click **Register at Domain**.
3. From the **Domain Control** menu, select **Register Proxy at Domain**.

If the Kerberos service name is changed later, you must rejoin the Barracuda NextGen Firewall F-Series to the domain in order to successfully use MS-CHAP v2 authentication again. If you want to use Kerberos with the new service name, you must re-register and restart the proxy.

Step 3. Create ACLs

To specify administration rights, you can implement access control for specific users. The Kerberos access control list (ACL) file, kadm5.acl allows you to specify individual privileges. You can also use the '*' wildcard in the principal name to specify group privileges. For more information, see Access Control.

Step 4. Configure your Web Browser

To use Kerberos authentication, you must specify the proxy settings in your web browser.

In the HTTP proxy settings for your web browser, enter the Kerberos service name (fully qualified domain name). For example: `01ha.domain.com`

> Do not enter an IP address in your HTTP proxy settings.

Kerberos Authentication through the Remote Management Tunnel

To allow remote F-Series Firewalls to connect to the authentication server through the remote management tunnel, you must activate the outbound **BOX-AUTH-MGMT-NAT** Host Firewall rule. By default, this rule is disabled.

Troubleshooting

To troubleshoot any issues with your Kerberos authentication settings, consider the following:

- Hostnames must be DNS-resolvable in both directions.
- Clock synchronization is crucial. The maximum allowed clock skew is 300 seconds.
- The Kerberos Constraint Delegation (KCD) service must be reachable for the system and the authenticating user.
- Service Principal Names (SPNs) are unique and available in the KDC´s database. If not, the KDC will not issue the TGS.
- To look up the ticketing process from your Windows client, you can use the `klist` command.
- To view log files, click the **Logs** tab on your Barracuda NextGen Firewall F-Series.
- If you see an error message containing **"BH hostname error"** in the HTTP Proxy service **cache.log**, check if the hostname is DNS-resolvable.
  `helperStatefulHandleRead:unexpected read from negotiateauthenticator #1, 18 bytes 'BH hostname error'`
- If you are using CNAME DNS records for your KDC and you see the following error message in the HTTP Proxy service **cache.log**. Use A DNS records instead.
  `ERROR: Negotiate Authentication validating user. Error returned 'BH received type 1 NTLM token'`