What is SMB barring?

It is a highly requested customer feature that was introduced with HNAS OS v13.9. This feature enables administrators to maintain a list of rogue client IP addresses that are barred from SMB/SMB2.x/SMB3 access to the server.  Clients that cause SMB NTLM authentication failures by providing an incorrect password are automatically added to the list if the rate of failure is sufficient. Automatic barring of clients is enabled by default, and an event log is generated when a client is barred.

No initial configuration of the feature is required; however the barred clients list can be managed if necessary using the following commands:

smb-barred-client-add

smb-barred-client-remove

smb-barred-clients-list

smb-barred-clients-clear

Clients are barred based on their IP address so each IPv4 and IPv6 (if configured) address will need to be considered a separate entry. Once a client is barred, it is not possible for that client to connect over SMB regardless of the credentials being used – manual removal from the ‘barred’ list would be required.

What are SMB barring benefits:

HNAS OS SMB barring feature is a free security enhancement (available to all customer with support contract) to protect HNAS cluster against denial of service (DoS) attack initiated by SMB client. When used conjunction with [NTLM authentication](https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/ntlm-user-authentication), it also improves SMB client quality of service.

NetApp offers similar capability to protect against DoS attack at extra cost if you subscribe to their services; see NetApp cloud Insights documentation:

A screenshot of a website

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

Why is this SMB barring was introduced?

* COVID-19 pandemic changes the work practice in the enterprise, more employees work remote which in turn, increase the risk for SMB client sessions to be exploited by “man-in-the-middle” attack.
* With IT budget squeeze and shrinking maintenance windows, we have seen rise in customer incidents that could have been avoided if authentication best practices had been implemented; IT operation too frequently deferred good hygiene due to its disruptive nature to avoid negotiating needed outages.
* As an example, customers that are still using NTLM authentication mechanism whereby HNAS authenticates users on their behalf, used when clients mount SMB shares using a short hostname [\\evs\share](file:///evs/share" \o "file://evs/share) (in contrast to Kerberos authentication, when clients authenticate directly with AD server, if they access HNAS using long FQDN as in [\\evs.acme.com\share](file:///evs.acme.com/share" \o "file://evs.acme.com/share)).
* Legacy NTLM authentication is supported with HNAS but is not as resilient with edge scenarios since HNAS acts as a proxy server in this method.
  1. NTLM authentication requires redirect of SMB client session authentication to local Microsoft Active domain controller; a burst of these requests with incorrect password (e.g. boot storm) could be perceived by the domain controller as DoS attack (if incident exceed lockout attribute threshold) which in turn will lockout the HNAS cluster and interrupt all SMB clients (see [Microsoft Active Directory account lockout](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsocial.technet.microsoft.com%2Fwiki%2Fcontents%2Farticles%2F32490.active-directory-bad-passwords-and-account-lockout.aspx&data=05%7C01%7CAl.Hagopian%40hitachivantara.com%7Cdb76fa35b8ef49e07acc08db581bc1d4%7C18791e1761594f52a8d4de814ca8284a%7C0%7C0%7C638200648466040215%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=lqmc7izFEa%2F4GehYxo5aON9Ay7yZnlCJE7XJzIYlmCs%3D&reserved=0" \o "https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsocial.technet.microsoft.com%2Fwiki%2Fcontents%2Farticles%2F32490.active-directory-bad-passwords-and-account-lockout.aspx&data=05%7C01%7CAl.Hagopian%40hitachivantara.com%7Cdb76fa35b8ef49e07acc08db581bc1d4%7C18791e1761594f52a8d4de814ca8284a%7C0%7C0%7C638200648466040215%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=lqmc7izFEa%2F4GehYxo5aON9Ay7yZnlCJE7XJzIYlmCs%3D&reserved=0)).
  2. If a client-supplied password is incorrect, the local Microsoft Active Directory domain controller will tear down a connection and HNAS will have to retry and reconnect to the domain controller for every bad password attempt. Meanwhile If that happens a lot, a backlog of valid client connection requests doesn’t get authenticated and will experience slower response time.
* Since NAS and active domain administration responsibility often fall in different departments, this risk often falls below the radar, and little is done proactively to avoid these edge cases.
* With NTLM authentication, SMB barring feature enables NAS administrator to eliminate the above-mentioned DoS attack risk, improve valid SMB client session quality of service and ensure communication resilience between HNAS cluster and local domain controller.
* Alternatively, for environment as described above, administrator can monitor SMB client sessions traffic with invalid password is below local domain controller account lockout threshold and/or increase threshold value to avoid any service interruption.

SMB sessions with incorrect password can occur for a large number of reasons – some of which include:

* Attempted brute-force attacks;
* Service accounts with passwords that have been recently changed or have expired;
* Issues with Active Directory replication;
* Cached user credentials saved in certain programs;
* Stored login details that contain overlapping credentials;
* Scheduled tasks using expired credentials;
* Shared drives using expired credentials;