Allowing or Denying Client Certificates

https://campus.barracuda.com/doc/19333476/

The **TRAFFIC > Client Certificates** page allows you to define allow/deny rules based on Client Certificates. These settings are not used unless **Enable Client Authentication** is *Yes* for the Service on the **BASIC > Services** page under **Advanced Options**.

When Client Authentication is turned on for a service, all clients are required to present a certificate to access the website. The certificate is first checked for validity. A valid certificate cannot be expired, and must be signed by a certificate authority (CA) listed under Trusted Certificates for the service. Even a valid certificate signed by a trusted CA can be rejected based on the certificate attributes. This is useful when you wish to revoke an issued valid certificate.

How it works:

Each Allow/Deny rule has the following important attributes:

- A sequence number specifying the order in which to evaluate the rule.
- A set of attribute matches (like Certificate Serial number). The attribute can either be a wildcard match (*, to indicate match any value), or it can be a specific value, matching the certificate's corresponding attribute exactly.
- An action to take when the presented client certificate matches this rule.

When a request is received, the Client certificate is compared to all Allow/Deny rules in sequence number order, starting from the lowest sequence number. Each attribute in the rule is compared, and if all attributes match a rule, the corresponding action (Allow or Deny) is taken and no further rules are compared.

When no rule matches the Client Certificate in the request, the request is allowed by default.

To allow only requests whose Client Certificates match a rule, create a Deny rule with a high sequence number (10000, for example) which matches all rules (has * for all attributes) and the action **Deny**. Every request with a client certificate which fails to match a rule will be denied. Each allowed certificate must have a corresponding Allow rule with a lower sequence number.

> If you create a high sequence number Deny rule to deny all except explicitly allowed Certificates, a request will be allowed only if its Certificate and all Certificates in its chain match an Allow Rule. If its intermediate or Trusted Certificate does not match any rule, the request is denied.

Complex rules can be built using Allow/Deny rules. For example, to deny all certificates from the Sales

department except one that is identified by its serial number, create the following two rules:

- Sequence = 1; Action = Allow; Organizational Unit = Sales; Serial Number = 12345
- Sequence = 2; Action = Deny; Organizational Unit = Sales

While complex rules can be built if needed, the recommended configuration allows all certificates signed by a trusted CA and uses the Allow/Deny list only to revoke access for issued certificates that are no longer valid. The Certificate serial number can uniquely identify a Certificate issued by a single CA in the event that it must be revoked. The Common Name can also be used to identify a revoked Certificate.

Configuring Allow/Deny Certificate Rules

Detailed instructions for configuring Allow/Deny Certificate rules are available on the **TRAFFIC > Client Certificates** page by clicking **Help** on that page.

For a certificate to be allowed using an Allow Rule, ensure that Allow Rules also exist for all Certificates in its chain. If the Certificate itself matches an Allow Rule, but its intermediate or Trusted Certificate does not match any rule, the request is denied.