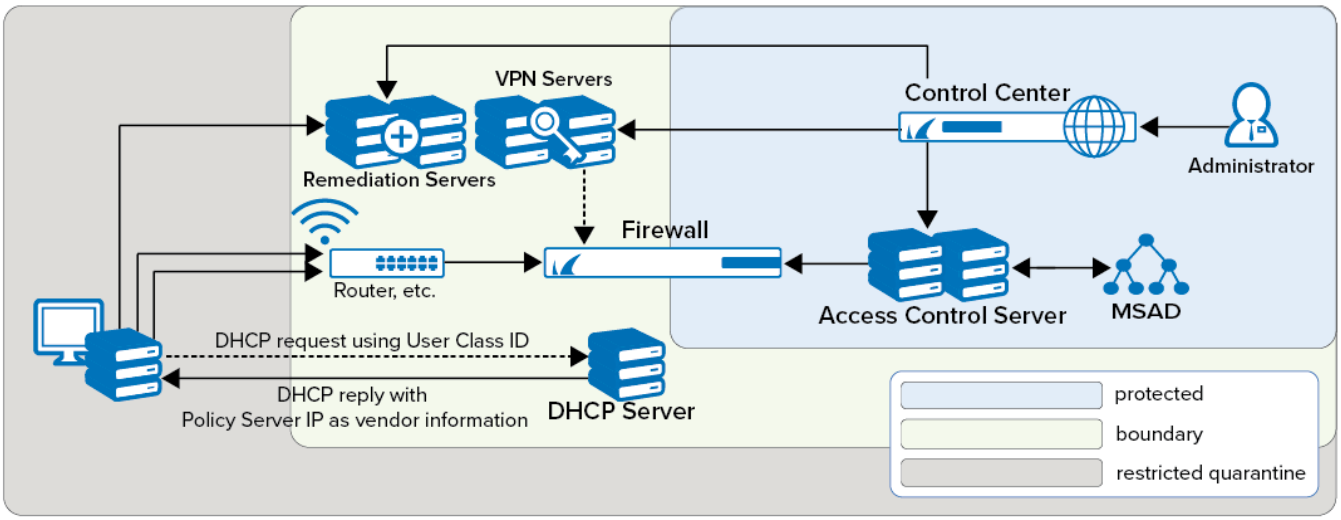
Deployment Options

https://campus.barracuda.com/doc/75696546/

The Barracuda Network Access Client can be used to implement an endpoint security policy on Windows-based endpoints within a corporate network. Policy enforcement is provided by the software installed on the endpoint and, with regard to enforcement outside the local collision domain, by Barracuda firewalls. The latter may interpret the access policy attribute assigned to the endpoint within their rulesets. This provides a way to enforce network access control concepts based on date and time, identity, and health state and type of network access.

Secure Network Desktop Connections



This setup requires the presence of at least one Access Control Service. This service entails two component services.

- The SHV is the policy matching engine that determines the applicable policy according to the connector's identity and current health state. The SHV issues a digitally signed cookie to the connecting endpoint that contains all the information pertinent to the identity and state of this client. The cookie serves as a passport of limited temporal validity with which the endpoint may identify itself to the remediation server.
- The remediation server is the component from which policy attributes, such as firewall rulesets, welcome messages, bitmaps, and client software components required for updates can be obtained. It can be run on the same Barracuda CloudGen Firewall system as the SHV or, for load balancing reasons, it can be spread out over several Barracuda CloudGen Firewalls.

SHV and remediation server must always remain accessible to all endpoints regardless of the currently active firewall ruleset.

The Access Control Service is automatically licensed on Barracuda CloudGen Firewalls. It is possible to equip all CloudGen Firewall branch office devices with a remediation server in order to reduce WAN traffic and optimize response times.

Since the Network Access Clients communicate with the Access Control Server in cyclic intervals, the Access Control Server should be placed as close as possible to the Network Access Clients. This helps reduce network traffic and improve response times.

Address Assignment

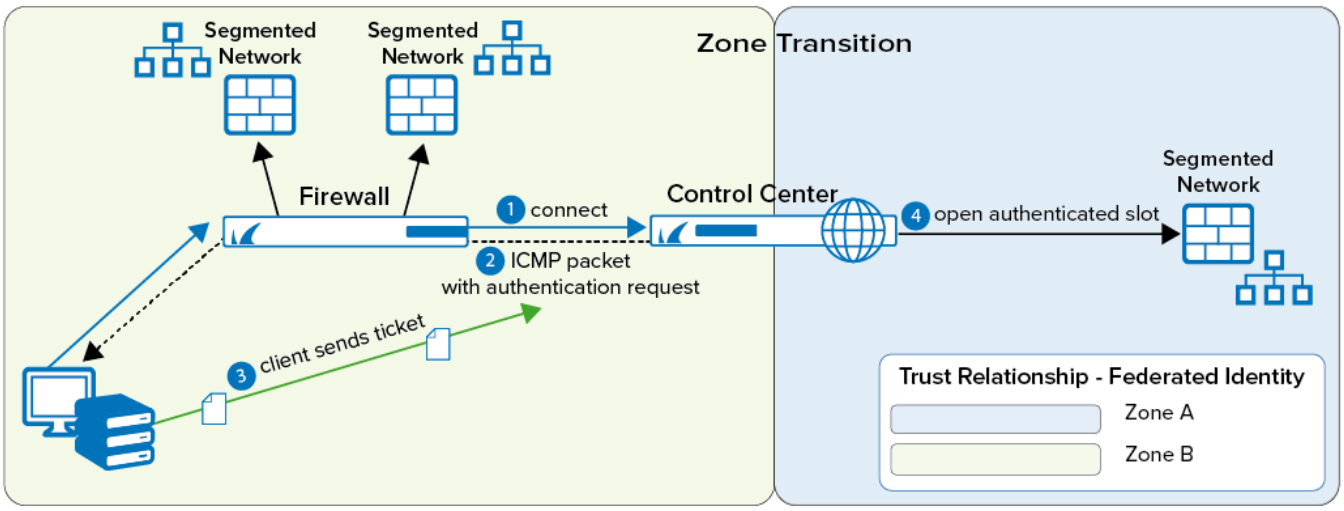
There are two options to let the client know at which address the SHV service component may be reached:

- The respective addresses are configured statically within the client configuration on the endpoint. This approach is mandatory if DHCP-based address assignment is not used.
- In the case of DHCP-based address assignment, the respective address or addresses are assigned to the client by way of the vendor ID DHCP option (43).

DHCP is also used to make a distinction between ist own endpoint systems with an installed client and the so-called guest systems. Because guest systems cannot communicate with SHV, they are not assigned any SHV addresses. By way of the DHCP user ID option sent by the client, a DHCP server may assign an address from a pool on a separate subnet.

The CloudGen Firewall as Border Patrol

Clients often need to access remote trust zones for which restricted access rights and stronger security measures apply. Consequently, the means to assess the suitability of crossing clients to access target trust zones needs to be available. The border patrol validates the credentials of crossing clients, including authentication and health status data, so that the applicable security measures are correctly met. Trust zones need to have a consistent and up-to-date view of the client's authentication information that is shared across the whole network. The CloudGen Firewall ensures that changes are replicated and synchronized across the various available servers and databases, so that identity federation is achieved.



The authentication process is based on the use of ICMP packages. The client submits an access request. The border patrol responds by sending an authentication request through an ICMP package. Then, the client replies with a ticket containing the cookie issued by the remediation service in the trust zone of origin and its corresponding access rights. If health status and permission match the minimum requirements of the target trust zone, the client is granted access. If the border patrol denies the request, no remediation will be available. Access is either granted or fully denied.

Secure Mobile Desktop Connections

The Barracuda Network Access Client can be used to secure mobile desktops connecting to the corporate LAN through the Internet. The integrated VPN client will establish a secure connection to a Barracuda CloudGen VPN service. The Network Access Monitor will then communicate with the responsible SHV through the VPN tunnel. From this point on, the overall procedure is quite analogous to the LAN scenario. The VPN server fully controls the virtual connection. That means that traffic within the VPN network's collision domain is also fully subject to the Network Access Control framework.

Figures