Firewall Integrations

Firewalls offers important security benefits for a campus networks, but they are also an easy target for a DoS attack (intentional or unintentional) because of session limits or things that can't be offloaded and ends up on the CPU etc.

One option to try and get the best of both worlds might be to utilize both Firewalls and ACLs in conjunction by implementing some form of policy-based redirect (Arista MSS Macro-Segmentation Services or Cisco Service Graphs with Policy-based redirect), basically classic policy-based routing (PBR).

One example implementation might be:

1. Implement L3 anycast gateway for client networks in campus switches
2. Set up linknet to Firewall in same VRF as client networks
3. Create ACLs on client SVIs that matches and redirects all traffic ***except*** HTTPS/TCP 443 the firewall linknet, traffic to local DNS server should probably also not be redirected to firewall
4. ACLs for return traffic so firewall is not confused from asymmetric routing, block non-established/SYN HTTPS to client networks

Advantages:

1. Clients should get excellent performance for HTTPS (most applications today?)
2. Clients will still be able to access most internet resources (HTTPS+DNS) even if the firewall is down/overwhelmed from DoS
3. Firewalls can't really do much with encrypted HTTPS traffic except checking certificate CN/SAN name anyway, so it doesn't help much to sending all that data via the firewall?
4. Stateful traffic that can't be handled via ACL (like UDP traffic) is still sent via firewall, protocols that are not as well-known/polished as HTTPS still sent via firewall

Disadvantages:

1. Clients can send any TCP protocol (not just HTTPS) via port 443 and avoid the firewall
2. No firewall logs for HTTPS traffic (Netflow/sflow instead?)
3. Harder to troubleshoot when different protocols/applications are routed different ways
4. Can't be used if you require NAT