SOFTEL
enabling networks

Deployment of Radware Defense Pro

To one of our clients, we have implemented DDoS solutions in their Data Center and Disaster Recovery Sites. They had the requirement to prevent their infrastructure from cyberattack that tries to make their website or network resources unavailable.

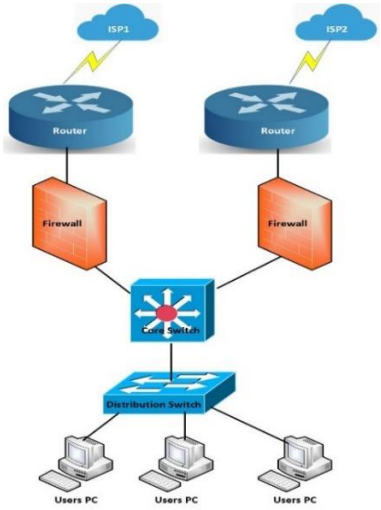
SCOPE

Solution required to be implemented at Data Center and Disaster Recovery sites, respectively. Customer is keeping the critical data which is very crucial. They want to protect these data from attacks like DDoS attacks – SYN floods, Low and slow, HTTP floods, SSL encryption, Brute force, BGP table attacks, Session attacks etc.

THE CHALLENGES

CUSTOMER was facing problem to secure their infrastructure from large volume of network attacks like DDoS attacks – SYN floods, Low and slow, HTTP floods, SSL encryption, Brute force, BGP table attacks, Session attacks etc. Major challenge was to provide the desired services and quick response to legitimate users for their requests.

CUSTOMER requirement was to deploy the solution with minimum configuration and topological changes with minimum downtime. The earlier solution used by the CUSTOMER to mitigate attacks were of multi-vendor. The inter-operability of those solution to responds against any attacking situation on the network infrastructure was a big challenge. Before deployment their deployed infrastructure was as follows -

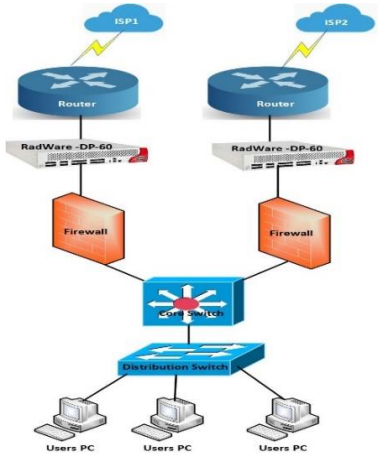


ANALYSIS & SOLUTION

We proposed Radware Defense Pro (DP-60) with Management Device APSolute as a solution, which has capability to secure Infrastructure from large volume of network attacks. To serve this purpose we installed Defense Pro Appliances in the In-line mode with-in the running IT Infrastructure of the CUSTOMER on both the Locations i.e. at Data Center Site as well as Disaster Recover Site. Deployed the appliance before firewall i.e. to stop attacks at perimeter level. We have resolved all the below challenges that were faced by the Customer

- DDoS – Attack
- SYN – Flood Attack
- HTTP Flood Attack
- Security from unwanted packets flows
- Brute Force Attack
- Smart SSL Attack
- Low and Slow applications response
- Busy Target Problem
- Behavioral based detection

After Solution deployment the network infrastructure Scenario at Data Center and Disaster Recovery site was as follows –



CONCLUSION

Solution is successfully deployed at Data Center and Disaster Recovery Site Locations. Customer personnel are trained enough to make policies and manage the appliances in a professional manner. The solution was deployed with the minimum downtime and no major configuration changes. The Solution deployed in High Availability mode on both the locations to avoid the device failure scenario.

It removes the pain point of the CUSTOMER and easily monitors the flow of the network traffic with the behavioral analysis of the flow of packets.