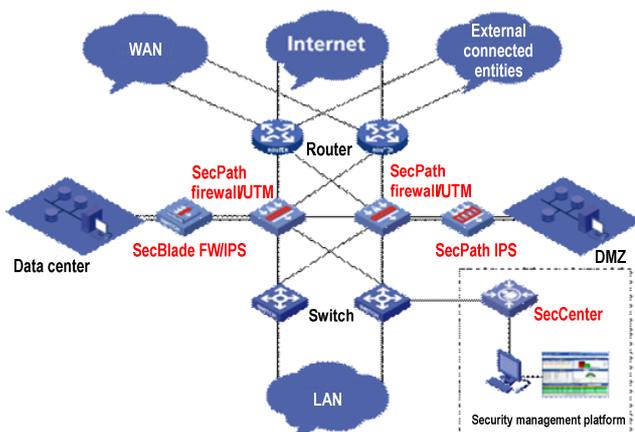# H3C Border Protection Solution

I. Overview

When a network is divided into different security zones, network borders are formed between the security zones of different trust levels. A variety of attacks may occur across network borders and cause huge damage. Although traditional security protection measures, such as firewalls, antivirus software and IDS are taken at network borders, the following issues still harass users:

- How to deal with attacks that keep emerging day after day, such as DDoS attacks, viruses, worms, and illegal modification of pages?
- How to implement the unified security management of the devices and staff that keep increasing day after day?

H3C border protection solution can thoroughly solve the above issues. It is the optimal solution for border security protection. The solution consists of the security gateway, the intrusion prevention system, and the security management platform. The security gateway (SecPath firewall/UTM) integrates L2-L4 packet filtering and stateful inspection technologies, and cooperates with the SecPath IPS L4-L7 intrusion prevention system to provide comprehensive L2-L7 security protection and effectively defend against attacks, such as illegal access, viruses, worms, and illegal page modification. The security management platform manages the security gateway, the intrusion prevention system, and the network equipment in a centralized way.

II. Typical Deployment

III. Solution Features

The Most Comprehensive Border Security Protection

H3C launched the SecBlade firewall/IPS module and the SecPath firewall/IPS box equipment based on the core switch. H3C is the only vendor in the industry that can provide both 10GE cards and box equipment, and can provide solutions in two product forms according to the specific user requirements.

The SecPath/SecBlade firewall integrates packet filtering and stateful inspection technologies and defines different security policies for the security zones of different trust levels to prevent unauthorized access. The SecPath box equipment supports H3C Open Application Architecture (OAA). Service modules, such as the antivirus module and the network stream analysis module, can be deployed on the equipment. The SecPath/SecBlade IPS is the only IPS product in the industry that integrates a vulnerability database, a virus database, and a protocol database. The feature library contains up to ten thousand types of features that keep updating and can exactly identify network attacks in real time, such as worms, viruses and Trojan Horses. The SecPath UTM provides numerous security functions, including virus prevention, URL filtering, vulnerability and attack prevention, junk mail prevention, P2P/IM application layer traffic control, and user behavior audit, in addition to the traditional firewall, VPN, and NAT functions.

H3C provides comprehensive L2-L7 security protection for users through an organic combination of the firewall and IPS. The border protection solution can effectively guard against various security risks from network borders.

Unified Security Management

As there is no information exchange between different types of network and security devices, isolated information islands may easily occur. The SecCenter can manage network and security devices in a centralized way. It outputs analysis reports in real time after collecting, analyzing, correlating, summarizing, and uniformly processing bulky information, so as to help the administrator timely learn the security status of the existing

network and help the administrator make analysis and decisions.

ʊ Deep Integration of Security and Networks

H3C has accumulated rich technical experience in the network and security fields. Users can select to add the 10GE SecBlade firewall/IP module to the core switch. The 10GE SecBlade firewall/IP module provides complete security protection to meet the border isolation requirements of large-scale campus networks and internal areas, whereas no separate security equipment needs to be deployed. This simplifies the network structure, avoids single-point failures, facilitates management, and really implements the deep integration of security and networks.

ʊ High Reliability

H3C equipment employs advanced technologies, such as 1+1 hot backup and L3 Monitor to implement 1+1 link backup and 1+1 gateway backup. When a link or a device fails, the system can timely discover the failure and perform automatic switching in a short time, thus greatly improving the network reliability and guaranteeing the uninterrupted running of user services.

ʊ Virtual Security Service

H3C SecPath firewall, UTM, and IPS products can provide the virtual security service. Multiple virtual systems are defined to separately deploy security policies for the multiple services of a user. When the user's services change or a new service department is established, you can add or delete virtual systems to flexibly solve the subsequent network expansion requirements. This simplifies network management and effectively reduces the user's security construction cost.

IV. Order Information

Model	Description
SecPath/SecBlade Firewall	Solves border isolation and security requirements.
SecPath/SecBlade IPS	Solves L4-L7 intrusion prevention requirements.
SecPath UTM	Solves the security requirements of small- and medium-scale users.
SecCenter	Collects and analyzes network security events, and outputs security audit reports.

IP network