



Role Based Network Services

1. Introduction

Traditional firewalls use the concept of security zones to segment a physical network into different domains, each with different security properties and requirements. The device connecting to a physical domain assumes the responsibility of security enforcement for the domain. Other security and network equipments are mostly using IP for monitoring and management.

With the development of network technology, there are more and more ways users can connect to the network. The same company employee, can use the office PC at one time, use his laptop from a conference room through wireless network at another. He can also remote access the company network at home or when traveling. In this case, the traditional ways of management based on IP is not enough. Furthermore, even the same PC with same IP may have different access rights depending on its health conditions.

Hillstone security appliances support Role Based Network Services (RBNS). It combines user's identity, group information, his way of accessing the network, PC health status to determine the network service that the user can access, results in fine grained control of the dynamic network.

RBNS, when applied to firewall is Role Based Access Control (RBAC).

Acronyms	Full Term
RBNS	Role Based Network Services
IPBNS	IP Based Network Services
RBAC	Role Based Access Control
ACL	Access Control List
DDNS	Dynamic Domain Name Server

Role Based Network Services

2. Access Control Based on IP

Traditional firewall use policies or ACLs that permit or deny traffic based on the low level characteristics of the traffic. The characteristics that common firewall policy relies on are source IP address, source IP port, destination IP address, destination IP port, protocol or application. Usually the policy is bounded to an interface. Some company introduce the concept of security zones as a group of interfaces. The set of policies is defined across ingress security zone and egress security zone. Firewall policies follow the “first match” principle. The following is an example:

Src zone	Dst zone	Src IP	Src port	Dst IP	Dst port	prot	group	action
Trust	Untrust	Any	Any	www.test.com	80	TCP	g1	deny
Trust	Untrust	Any	Any	Any	Any	TCP	g2	permit
Trust	DMZ	10.1.1.1	Any	1.1.1.1	Any	Any	-	permit
Untrust	DMZ	Any	Any	1.1.1.1	80	TCP	-	permit

With given source zone and destination zone, some company introduce the concept of user group. If the flow been inspected match the policy, with user identified with firewall authentication, the policy will determine whether the flow is permitted based on whether user is within the group or not.

But because of the firewall policy is “first match” , if the user is not in the group of the first matched policy, the flow will be denied, even if there is another policy match after it. With the above example, if there is an user that belongs to group g2 visiting www.test.com, because based on IP-port 5-tuple match, the first policy is matched, we will only use this policy to match group information. Even if the group does not match, we will not continue to search other firewall policies.

3. Role Based Network Services

Hillstone Role Based Network Services (RBNS) consists of 3 parts:

- User authentication and identification
- User role determination
- Role based control and management

1.1 User Authentication and Identification

The first step of RBNS is identification of the user identity. Most companies already



Role Based Network Services

have AAA mechanism already in place. Hillstone RBNS can cooperate with these AAA mechanisms. For example, user log on and group information can be dynamically obtain from Active Directory Servers such as Microsoft Windows 2003.

Hillstone devices also can authenticate users using access authentication through the device, using company servers as backend. Hillstone device support local users and user groups. Today, users can be identified in the following ways:

- Interop with Active Directory and other standard AAA server to obtain log on information
- 802.1x
- HTTP Authentication
- SSL VPN
- IPSec VPN
- Static Binding

1.2 Determine of User Roles

After a user is authenticated and identified, user can be assigned one or more roles. Roles is like a token, a flow with different token will get different treatment during processing. User roles can be determined by one or more of the following elements:

- User name
- User group that user belongs to
- User IP
- Security Zone user is accessing from
- User ways of connecting
- User PC System
- User PC security status
- A combination of other roles

The role of the user determine who the user is (Who), where he is accessing from (Where), how he is connected (How). This together with time schedule (When), can achieve fine grained control the behavior (What) of the user.

1.3 Role Based Network Services

Hillstone device support a rich set of network service based on user identities:

- Role Based Access Control: Support in firewall policies

Role Based Network Services

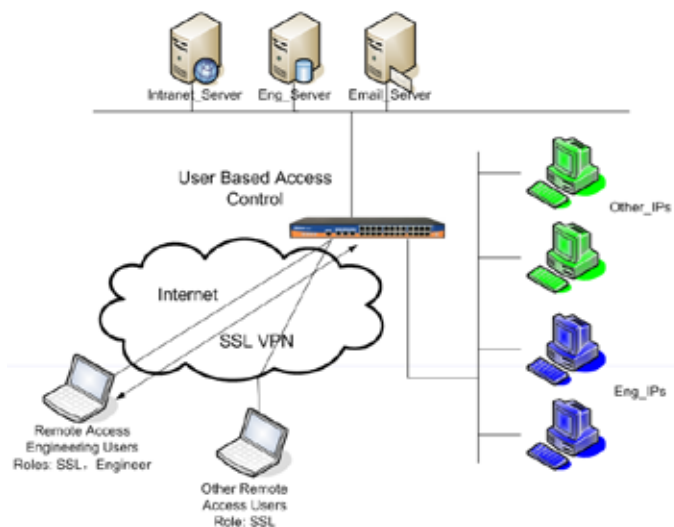
- Role Based QoS: Bandwidth control based on user roles
- Role Based Session Number Control
- Role Based Application Control and Content Control, including AV and IPS
- Role Base Network Behavior Control

1.4 Role Based Access Control (RBAC)

In data processing, Hillstone device uses port information, security zone, VPN, IP information to identify the user and the roles that the user have. We utilize the role information in searching for security policies. Using firewall policy as an example, the searching for firewall policy is no longer based on IP 5-tuple, but a 6-tuple including user roles. The characteristics of this technology are:

- Support the mix of regular firewall policies and role based policies at the same time. As with regular firewall, using the natural policy order to determine the priorities of the policy.
- Fully compatible with firewall policy. Each policy could have a role “Any” , which matches all user. A policy with role “Any” degenerated into a regular firewall policy.
- Policy match uses 6-tuple including user roles. “First match” principle of the firewall is still followed.
- Support users with multiple roles. But roles have no priority. The matching is based on natural order of the policies.

The following is an example



Role Based Network Services

Role	Src IP	Src port	Dst IP	Dst port	prot	action
SSL	Any	Any	Intranet_Server	Any	Any	deny
Engineer	Any	Any	Eng_Server	Any	Any	permit
Any	Eng_IPs	Any	Any	Any	Any	permit
Any	Any	Any	Email_Server	Any	Any	permit

With above example, a company's security gateway have firewall and SSL VPN functionality. When user uses SSLVPN to access the network, system will assign a role to these traffic – “SSL” . For Engineersthat access remotely, the system assign another role – “Engineer” . The company PC are divided into two categories: one kind uses by engineers, with IP address grouped in “Eng_IPs” , the other kind used by everyone else. The company have 3 servers: Email Server, Intranet server and Engineering Server.

The policy list reflects the access policy of the company:

- Remote access users through SSL VPN can not access Intranet Server
- Engineers can access Engineering Server either through remote access SSL VPN or within the company.
- Engineers when accessing through intranet PC can access all servers.
- Everyone else can access Email server to read their email, either through remote access SSL VPN or through intranet PC

4. Conclusion

Hillstone appliance support next generation network service based on user roles. The roles can be based on user, his location, his way of access and PC status. Together with scheduling and application control functionality already comes with the appliance, can provide truly control over 5 elements (Who, Where, When, What and How) of network events.