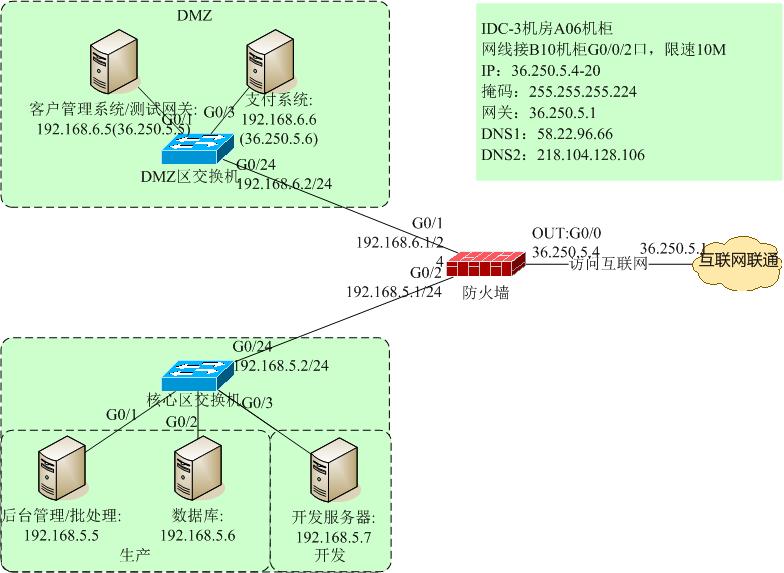
通宝易网络系统集成方案

1. **整体架构说明**

通易宝网络系统包含三个区域：outside区域，连接互联网，安全级别为0；DMZ区域，连接前置web服务器（含客户管理系统，支付网关）；inside区域，连接应用服务器，数据库服务器，开发服务器。详细拓扑结构见下图：



防火墙采用思科ASA5515，配置为路由模式，并提供DMZ区服务器的NAT功能。交换机采用华三S5120作为核心交换机。

1. **权限说明**

目前只开放了DMZ区两台服务器的http公网访问权限。其他权限未开通。

各区域间访问权限如下：

核心区可以访问DMZ/outside区域，可以连接到公网的ip地址，不能通过域名访问互联网。

DMZ无法访问核心区，可以连接到公网的ip地址，不能通过域名访问互联网。

Outside（公网）可以访问DMZ区两台服务器的http端口。

1. **网络设备配置规范**

## 设备命名规则



AAA-BB\_CC-H\*\*\*\_\*

设备标识由管理属性和物理属性两部分组成，两者之间用减号“－”隔开，这些属性具体又分为五个字段，具体说明如下：

|  |  |  |
| --- | --- | --- |
| **编号** | **作用** | **说明** |
|  | 机构标识 | 用于标识数据中心（软件园）。原则上由两个字母组成，取机构名称英文或拼音缩写。定义如下：  通易宝：TBY |
|  | 应用功能区标识 | 用于标识数据中心各功能模块区设备。原则上由两个字母组成，取应用功能区英文或拼音缩写。定义如下：  DMZ区域：DMZ  核心区：CORE |
|  | 设备功能类型标识 | 原则上由二个字母组成，用于标识设备功能类型。定义如下：  核心交换机：CS（Core Switch）  汇聚交换机：AS（Aggregate Switch）  防火墙：FW（FireWall） |
|  | 厂商型号标识 | 原则上由一个字母和若干数字或字母组成，字母用于标识设备厂商，数字及其后的字母为设备型号系列标识。字母定义如下：  CISCO：C  华为/H3C：H  数字及其后的字母用于标识设备具体的型号系列，如Cisco ASA5515取ASA 5515，H3C S5120取5120 |
|  | 同类型设备编号 | 原则上是一位整数，用于标识同类型设备数量编号 |

## 设备命名

|  |  |
| --- | --- |
| 设备标识 | 备注 |
| TBY-\_FW-ASA5515\_1 | 思科核心防火墙ASA5515 |
| TBY-DMZ\_CS-H5120\_1 | DMZ区核心交换机华三 S5120 |
| TBY-CORE\_CS- H5120\_1 | 核心区交换机华三S5120 |

## 接口命名规则

接口标识由对端设备及接口两部分组成，两者之间用减号“：”隔开，这些属性具体又分为三个字段，具体说明如下：AA:设备所属区域；BB：设备名称；CC：接口。示例如下：\*\*\*To AA\_BB:CC\*\*\*

## IP地址规划

在地址规划中，定义了两个C类地址作为DMZ区服务器和核心区服务器的接入地址，内部互联通过一个29位地址段实现，便于后续设备的扩容使用。防火墙对外的ip地址由运营商提供。详细分配如下：

|  |  |
| --- | --- |
| **核心区(192.168.5.0/24,GT:192.168.5.1)** | |
| **设备名称** | **IP** |
| 后台管理系统(BMS) | 192.168.5.5 |
| 数据库(DB) | 192.168.5.6 |
| 开发服务器(DS) | 192.168.5.7 |

|  |  |
| --- | --- |
| **DMZ区(192.168.6.0/24,GT:192.168.6.1)** | |
| **设备名称** | **IP** |
| 客户管理系统（CMS） | 192.168.6.5-36.250.5.6 |
| 支付网关(PAYGT) | 192.168.6.6-36.250.5.5 |

|  |  |  |  |
| --- | --- | --- | --- |
| **设备互联接口** | | | |
| **设备名称** | **接口** | **描述** | **IP** |
| TBY-DMZ\_CS-H5120\_1 | G1/0/24 | To TBY-\_FW-ASA5515\_1: G0/1 | 192.168.6.2 |
| TBY-DMZ\_CS-H5120\_1 | G1/0/1 | To DMZ\_CMS |  |
| TBY-DMZ\_CS-H5120\_1 | G1/0/2 | To DMZ\_PAYGT |  |
| TBY-CORE\_CS- H5120\_1 | G1/0/24 | To TBY-\_FW-ASA5515\_1: G0/2 | 192.168.5.2 |
| TBY-CORE\_CS- H5120\_1 | G1/0/1 | To Core\_BMS |  |
| TBY-CORE\_CS- H5120\_1 | G1/0/2 | To Core\_DB |  |
| TBY-CORE\_CS- H5120\_1 | G1/0/3 | To Core\_DS |  |
| TBY-\_FW-ASA5515\_1 | G0/0 | To Internet | 36.250.5.4 |
| TBY-\_FW-ASA5515\_1 | G0/1 | To TBY-DMZ\_CS-H5120\_1:G1/0/24 | 192.168.6.1 |
| TBY-\_FW-ASA5515\_1 | G0/2 | To TBY-CORE\_CS- H5120\_1:G1/0/24 | 192.168.5.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NAT地址对应表** | | | | |
| **设备名称** | **源IP** | **源端口** | **目的IP** | **目的端口** |
| 客户管理系统（CMS） | 192.168.6.5 | ANY | 36.250.5.5 | ANY |
| 支付网关(PAYGT) | 192.168.6.6 | ANY | 36.250.5.6 | ANY |

1. **网络设备配置：**
2. **TBY-\_FW-ASA5515\_1**

hostname TYBFWASA5515

enable password gUweSTfBSkqzMVWM encrypted

passwd gUweSTfBSkqzMVWM encrypted

names

ip local pool vpn\_pool 192.168.8.5-192.168.8.100 mask 255.255.255.0

!

interface GigabitEthernet0/0

description \*\*\* To Internet \*\*\*

nameif outside

security-level 0

ip address 36.250.5.4 255.255.255.224

!

interface GigabitEthernet0/1

description \*\*\* To TYB-DMZ\_CS-H5120\_1:G1/0/24\*\*\*

nameif DMZ

security-level 50

ip address 192.168.6.1 255.255.255.0

!

interface GigabitEthernet0/2

description \*\*\* To To TYB-CORE\_CS- H5120\_1:G1/0/24\*\*\*

nameif inside

security-level 100

ip address 192.168.5.1 255.255.255.0

!

interface GigabitEthernet0/3

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/4

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/5

shutdown

no nameif

no security-level

no ip address

!

interface Management0/0

management-only

nameif management

security-level 100

ip address 192.168.1.1 255.255.255.0

!

banner login WARNING: Unauthorized access are forbidden! All of your behaviors will be recorded!

boot system disk0:/asa912-smp-k8.bin

ftp mode passive

clock timezone BJT 8

object network CMS

host 192.168.6.5

object network NETWORK\_OBJ\_192.168.8.0\_25

subnet 192.168.8.0 255.255.255.128

object network CMS\_NAT

host 36.250.5.5

object network test\_host

host 192.168.5.252

object network PAYGT\_NAT

host 36.250.5.6

object network PAYGT

host 192.168.6.6

object network vpn\_pl

subnet 192.168.8.0 255.255.255.0

object network ToInternet

host 36.250.5.20

object-group network DM\_INLINE\_NETWORK\_3

network-object object CMS

network-object object PAYGT

object-group network DM\_INLINE\_NETWORK\_1

network-object 192.168.5.0 255.255.255.0

network-object 192.168.6.0 255.255.255.0

object-group network DM\_INLINE\_NETWORK\_2

network-object 192.168.5.0 255.255.255.0

network-object 192.168.6.0 255.255.255.0

access-list DMZ\_access\_in extended permit ip 192.168.6.0 255.255.255.0 object vpn\_pl

access-list outside\_access\_in extended permit tcp any object-group DM\_INLINE\_NETWORK\_3 eq www

access-list inside\_access\_in extended permit ip 192.168.5.0 255.255.255.0 object vpn\_pl

access-list inside\_access\_in extended permit ip any any

access-list tyb\_vpn\_splitTunnelAcl standard permit 192.168.5.0 255.255.255.0

access-list tyb\_vpn\_splitTunnelAcl standard permit 192.168.6.0 255.255.255.0

access-list tby\_vpn\_splitTunnelAcl standard permit 192.168.5.0 255.255.255.0

access-list tby\_vpn\_splitTunnelAcl standard permit 192.168.6.0 255.255.255.0

pager lines 24

logging enable

logging timestamp

logging buffer-size 1048576

logging trap notifications

logging asdm informational

mtu outside 1500

mtu DMZ 1500

mtu inside 1500

mtu management 1500

no failover

icmp unreachable rate-limit 1 burst-size 1

icmp permit any DMZ

asdm image disk0:/asdm-713.bin

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

nat (outside,outside) source static any any destination static NETWORK\_OBJ\_192.168.8.0\_25 NETWORK\_OBJ\_192.168.8.0\_25 no-proxy-arp route-lookup

nat (inside,outside) source static DM\_INLINE\_NETWORK\_1 DM\_INLINE\_NETWORK\_1 destination static NETWORK\_OBJ\_192.168.8.0\_25 NETWORK\_OBJ\_192.168.8.0\_25 no-proxy-arp route-lookup

nat (inside,outside) source static DM\_INLINE\_NETWORK\_2 DM\_INLINE\_NETWORK\_2 destination static NETWORK\_OBJ\_192.168.8.0\_25 NETWORK\_OBJ\_192.168.8.0\_25 no-proxy-arp route-lookup

nat (inside,outside) source static CMS CMS\_NAT

nat (inside,outside) source static PAYGT PAYGT\_NAT

access-group outside\_access\_in in interface outside

access-group DMZ\_access\_in in interface DMZ

access-group inside\_access\_in in interface inside

route outside 0.0.0.0 0.0.0.0 36.250.5.1 1

route inside 192.168.5.0 255.255.255.0 192.168.7.10 1

route DMZ 192.168.6.0 255.255.255.0 192.168.7.2 1

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00

timeout floating-conn 0:00:00

dynamic-access-policy-record DfltAccessPolicy

user-identity default-domain LOCAL

aaa authentication ssh console LOCAL

aaa authentication http console LOCAL

aaa authentication serial console LOCAL

http server enable

http 192.168.1.0 255.255.255.0 management

http 220.250.1.72 255.255.255.248 outside

http 202.109.197.192 255.255.255.248 outside

http 192.168.5.0 255.255.255.0 inside

http 192.168.6.0 255.255.255.0 DMZ

http 192.168.8.0 255.255.255.0 inside

no snmp-server location

no snmp-server contact

snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac

crypto ipsec security-association pmtu-aging infinite

crypto dynamic-map SYSTEM\_DEFAULT\_CRYPTO\_MAP 65535 set pfs group1

crypto dynamic-map SYSTEM\_DEFAULT\_CRYPTO\_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5

crypto map outside\_map 65535 ipsec-isakmp dynamic SYSTEM\_DEFAULT\_CRYPTO\_MAP

crypto map outside\_map interface outside

crypto ca trustpool policy

crypto ikev1 enable outside

crypto ikev1 policy 10

authentication crack

encryption aes-256

hash sha

group 2

lifetime 86400

crypto ikev1 policy 20

authentication rsa-sig

encryption aes-256

hash sha

group 2

lifetime 86400

crypto ikev1 policy 30

authentication pre-share

encryption aes-256

hash sha

group 2

lifetime 86400

crypto ikev1 policy 40

authentication crack

encryption aes-192

hash sha

group 2

lifetime 86400

crypto ikev1 policy 50

authentication rsa-sig

encryption aes-192

hash sha

group 2

lifetime 86400

crypto ikev1 policy 60

authentication pre-share

encryption aes-192

hash sha

group 2

lifetime 86400

crypto ikev1 policy 70

authentication crack

encryption aes

hash sha

group 2

lifetime 86400

crypto ikev1 policy 80

authentication rsa-sig

encryption aes

hash sha

group 2

lifetime 86400

crypto ikev1 policy 90

authentication pre-share

encryption aes

hash sha

group 2

lifetime 86400

crypto ikev1 policy 100

authentication crack

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 110

authentication rsa-sig

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 120

authentication pre-share

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 130

authentication crack

encryption des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 140

authentication rsa-sig

encryption des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 150

authentication pre-share

encryption des

hash sha

group 2

lifetime 86400

telnet timeout 5

ssh 220.250.1.72 255.255.255.248 outside

ssh 202.109.197.192 255.255.255.248 outside

ssh 192.168.5.0 255.255.255.0 inside

ssh 192.168.8.0 255.255.255.0 inside

ssh 192.168.1.0 255.255.255.0 management

ssh timeout 5

ssh version 2

ssh key-exchange group dh-group1-sha1

console timeout 0

management-access inside

dhcpd address 192.168.1.2-192.168.1.254 management

dhcpd enable management

!

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1

group-policy tby\_vpn internal

group-policy tby\_vpn attributes

vpn-tunnel-protocol ikev1

split-tunnel-policy tunnelspecified

split-tunnel-network-list value tby\_vpn\_splitTunnelAcl

username localadmin password AcdyFpZZtqiyMXTJ encrypted privilege 15

username tbydmz password Hx66VUcmiz4OQ4xg encrypted privilege 0

username tbydmz attributes

vpn-group-policy tby\_vpn

username user1 password iVl5fa5pZE5eZgL1 encrypted

username user1 attributes

vpn-group-policy tby\_vpn

username tbyinside password WKt/MmeKzZvaXt6C encrypted privilege 0

username tbyinside attributes

vpn-group-policy tby\_vpn

username hemz password 8dRejILFUX7/wNzH encrypted privilege 0

username hemz attributes

vpn-group-policy tby\_vpn

tunnel-group tby\_vpn type remote-access

tunnel-group tby\_vpn general-attributes

address-pool vpn\_pool

default-group-policy tby\_vpn

tunnel-group tby\_vpn ipsec-attributes

ikev1 pre-shared-key \*\*\*\*\*

!

class-map inspection\_default

match default-inspection-traffic

!

!

policy-map type inspect dns preset\_dns\_map

parameters

message-length maximum client auto

message-length maximum 512

policy-map global\_policy

class inspection\_default

inspect dns preset\_dns\_map

inspect ftp

inspect h323 h225

inspect h323 ras

inspect rsh

inspect rtsp

inspect esmtp

inspect sqlnet

inspect skinny

inspect sunrpc

inspect xdmcp

inspect sip

inspect netbios

inspect tftp

inspect ip-options

!

service-policy global\_policy global

prompt hostname context

no call-home reporting anonymous

Cryptochecksum:ab8658e0a6840c8979d85a6af0c2ea48

: end

1. **TBY-DMZ\_CS-H5120\_1**

sysname TYB-DMZ\_CS-H5120\_1

#

clock timezone BJT add 08:00:00

#

super password level 3 cipher $c$3$VlGgljdSCYScbEKnyltWgPNnhUtFSou/Z25bz5o=

#

irf mac-address persistent timer

irf auto-update enable

undo irf link-delay

#

domain default enable system

#

telnet server enable

#

password-recovery enable

#

vlan 1

#

vlan 20

#

vlan 21

description \*\*\*To Core Server\*\*\*

#

domain system

access-limit disable

state active

idle-cut disable

self-service-url disable

#

user-group system

#

local-user localadmin

password cipher $c$3$MHhn3NqXbdnl7/UnebZZdpMp4TbWHFBPaLhqAw4=

service-type ssh terminal

#

interface NULL0

#

interface Vlan-interface1

ip address dhcp-alloc client-identifier mac Vlan-interface1

#

interface Vlan-interface21

ip address 192.168.6.2 255.255.255.0

#

interface GigabitEthernet1/0/1

description \*\*\*To DMZ\_CMS:192.168.6.5\*\*\*

port access vlan 21

#

interface GigabitEthernet1/0/2

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/3

description \*\*\*To DMZ\_PAYGT:192.168.6.7\*\*\*

port access vlan 21

#

interface GigabitEthernet1/0/4

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/5

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/6

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/7

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/8

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/9

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/10

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/11

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/12

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/13

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/14

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/15

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/16

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/17

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/18

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/19

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/20

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/21

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/22

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/23

port access vlan 21

shutdown

#

interface GigabitEthernet1/0/24

description \*\*\* To TYB-\_FW-ASA5515\_1: G0/1\*\*\*

port access vlan 21

#

interface GigabitEthernet1/0/25

#

interface GigabitEthernet1/0/26

#

interface GigabitEthernet1/0/27

#

interface GigabitEthernet1/0/28

#

ip route-static 0.0.0.0 0.0.0.0 192.168.6.1

#

header login %

Warning: Unauthorized access are forbidden!//!//!

All of your behaviors will be recorded

%

#

ssh server enable

#

load tr069-configuration

#

user-interface aux 0

authentication-mode scheme

idle-timeout 5 0

user-interface vty 0 15

authentication-mode scheme

command accounting

idle-timeout 5 0

protocol inbound ssh

#

1. **TBY-CORE\_CS- H5120\_1**

sysname TYB-CORE\_CS-H5120\_1

#

clock timezone BJT add 08:00:00

#

super password level 3 cipher $c$3$wdGNw8uut3hh3nykhy0WiILvGToon/1roRzVUl8=

#

irf mac-address persistent timer

irf auto-update enable

undo irf link-delay

#

domain default enable system

#

telnet server enable

#

password-recovery enable

#

vlan 1

#

vlan 11

description \*\*\*To DMZ Server\*\*\*

#

domain system

access-limit disable

state active

idle-cut disable

self-service-url disable

#

public-key peer 192.168.5.1

public-key-code begin

30819F300D06092A864886F70D010101050003818D0030818902818100C6914C1619FE1A63

5436E4C3274E5B161C613359CBE144068359CE03F164BF09C3A71939CBB7AC1C312BBB05A3

F1D898AFD5A65D4F6C81D7B820E967B869031A5832DBAB205C3577AA97850D53969653720F

84D38532954F34D0C9D3449362561C59945D5B4C4FD240B3446645569D23F767F11CBCC749

FBB364865E0F94210B0203010001

public-key-code end

peer-public-key end

#

user-group system

#

local-user localadmin

password cipher $c$3$KQmKKjMd7+6q8bJYM6YRFvSNmyK/QsDGTd7DG2M=

service-type ssh terminal

#

interface NULL0

#

interface Vlan-interface1

ip address dhcp-alloc client-identifier mac Vlan-interface1

#

interface Vlan-interface11

ip address 192.168.5.2 255.255.255.0

#

interface GigabitEthernet1/0/1

description \*\*\*To Core\_BMS:192.168.5.5\*\*\*

port access vlan 11

#

interface GigabitEthernet1/0/2

description \*\*\*To Core\_DB:192.168.5.6\*\*\*

port access vlan 11

#

interface GigabitEthernet1/0/3

description \*\*\*To To Core\_DS:192.168.5.7\*\*\*

port access vlan 11

#

interface GigabitEthernet1/0/4

description \*\*\* To TYB-\_FW-ASA5515\_1: G0/1\*\*\*

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/5

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/6

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/7

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/8

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/9

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/10

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/11

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/12

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/13

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/14

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/15

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/16

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/17

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/18

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/19

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/20

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/21

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/22

port access vlan 11

shutdown

#

interface GigabitEthernet1/0/23

port access vlan 11

#

interface GigabitEthernet1/0/24

description \*\*\* To TYB-\_FW-ASA5515\_1: G0/2\*\*\*

port access vlan 11

#

interface GigabitEthernet1/0/25

#

interface GigabitEthernet1/0/26

#

interface GigabitEthernet1/0/27

#

interface GigabitEthernet1/0/28

#

ip route-static 0.0.0.0 0.0.0.0 192.168.5.1

#

header login %

Warning: Unauthorized access are forbidden!//!//!

All of your behaviors will be recorded

%

#

ssh server enable

ssh client authentication server 192.168.5.1 assign publickey 192.168.5.1

#

load tr069-configuration

#

user-interface aux 0

authentication-mode scheme

idle-timeout 5 0

user-interface vty 0 15

authentication-mode scheme

command accounting

idle-timeout 5 0

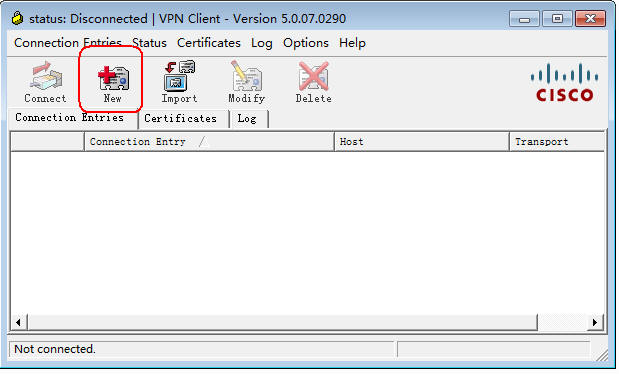
protocol inbound ssh

#

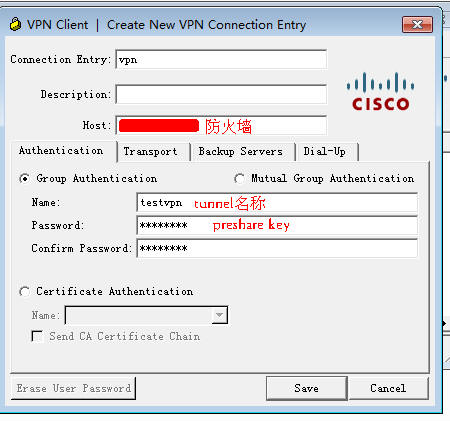
1. **cisco vpn client配置：。**

Tunnel name登陆的时候可以共用同一个名称。不同用户登陆可以选择不同的用户名。

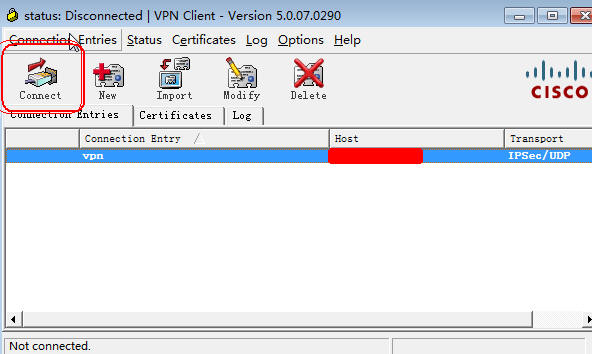
1. 新建一个vpn连接



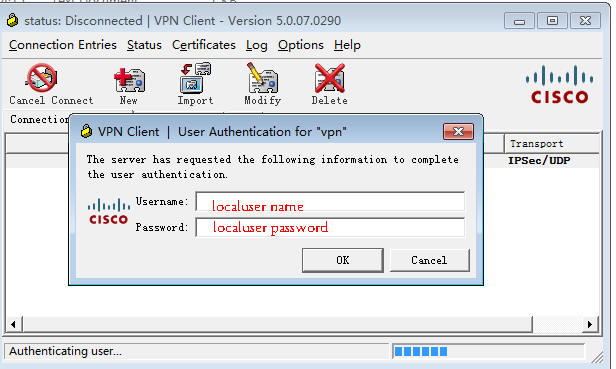
1. 配置tunnel 名称及预共享密钥，host填写的是防火墙outside接口的ip:36.250.5.4。



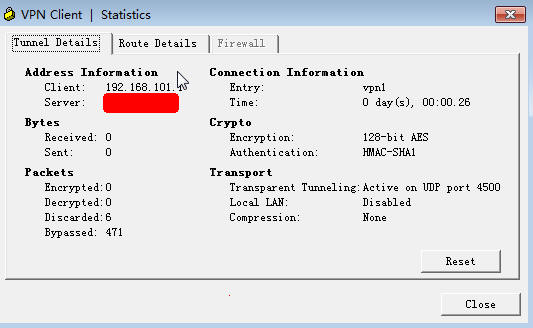
1. 点击connect



1. 填写新增的本地数据库用户。即可连接。



1. 连接后即可在客户端查看到相应的连接信息及路由信息。



1. **用户名密码：**

|  |  |  |
| --- | --- | --- |
| 通道 | 通道名 | Preshare-key |
| tby\_vpn | Tby@2014 |
| 本地用户 | 用户名 | 密码 |
| tbyinside | Inside\_2014 |
| user1 | user@pwd |
| tbydmz | Dmz@2014 |

用户名/密码：

tunnelname:tby\_vpn

preshare:Tby@2014

localuser:tbydmz

pwd:Dmz@2014

localuser:tbyinside

pwd:Inside\_2014

localuser:user1

pwd:user@pwd

vpnpool:192.168.8.5-100

mask:255.255.255.0