

PIX 515 - DHCP on WAN - Sample Script

Written by webadmin

Tuesday, 24 May 2011 21:46 - Last Updated Tuesday, 24 May 2011 22:23



PIX 515 - SETUP DHCP on WAN Interface & Sample Script

Suggested prerequisite reading:

» [Cisco Forum FAQ](#) » [Things to expect when setup network for home or small business](#)

For many cable and DSL internet connections, the ISPs inform their customers (subscribers) to set their router to receive IP address from them automatically. This means that the ISPs treat their subscriber's router as DHCP client.

When this is your case, then the following sample configuration is a good starting point to help you configure the firewall. There are two sample configurations provided here, one is the PIX version and another is ASA version. Note that both configurations are identical.

Typical network environment that might utilize following sample PIX/ASA configuration is as follows:

- * There is a modem in front of the PIX/ASA, which the modem connects to the ISP
- * ISP is providing Public IP address to the PIX/ASA via DHCP
- * There is NAT/PAT in place on the PIX/ASA to translate internal IP addresses to the ISP-provided Public IP address
- * The PIX/ASA is also acting as DHCP server to the local LAN, which provide dynamic IP info for hosts behind the PIX/ASA within the LAN

Note:

PIX 515 - DHCP on WAN - Sample Script

Written by webadmin

Tuesday, 24 May 2011 21:46 - Last Updated Tuesday, 24 May 2011 22:23

Keep in mind that there are two DHCP processes on this sample configuration. One is between your ISP and the PIX/ASA, and another is between the PIX/ASA and machines within your LAN. Your ISP would hand out specific WAN or Public IP address (i.e. 1.1.1.1) to the WAN interface of your PIX or ASA via ISP DHCP mechanism where your PIX/ASA would hand out completely different IP address for internal usage via PIX/ASA DHCP mechanism.

This sample PIX/ASA configuration assumes the followings

- * Internal private IP subnet (for hosts behind the PIX): 10.0.0.0/24
- * All of the hosts' gateway would be the PIX/ASA inside interface IP address: 10.0.0.1
- * The IP address range of 10.0.0.30-10.0.0.254 would be available for DHCP pool client
- * The IP address range of 10.0.0.2-10.0.0.29 would be reserved for statically-assigned hosts, consequently
- * The DHCP clients would also receive DNS IP addresses of 68.87.64.196 and 68.87.66.196 automatically as part of the dynamically assigned IP address process
- * When all hosts behind the PIX/ASA go out to the Internet, the hosts would be using the PIX/ASA outside interface IP address (which is the ISP-assigned Public IP address)
- * Necessary ICMP packet coming from the Internet would be permitted to enter your LAN

SAMPLE CONFIGURATION

1. PIX

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password ***** encrypted
passwd ***** encrypted
hostname PIX
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
object-group icmp-type ICMP-INBOUND
```

PIX 515 - DHCP on WAN - Sample Script

Written by webadmin

Tuesday, 24 May 2011 21:46 - Last Updated Tuesday, 24 May 2011 22:23

```
description Permit necessary inbound ICMP traffic
icmp-object 0
icmp-object 3
icmp-object 11
access-list INBOUND permit icmp any any object-group ICMP-INBOUND
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside dhcp setroute
ip address inside 10.0.0.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
access-group INBOUND in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no http server enable
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 10.0.0.30-10.0.0.254 inside
dhcpd dns 68.87.64.196 68.87.66.196
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable inside
terminal width 80
```

2. ASA

```
hostname ASA
domain-name xxxxx
enable password xxxxxxxxx encrypted
names
```

PIX 515 - DHCP on WAN - Sample Script

Written by webadmin

Tuesday, 24 May 2011 21:46 - Last Updated Tuesday, 24 May 2011 22:23

```
!  
interface Vlan1  
nameif inside  
security-level 100  
ip address 10.0.0.1 255.255.255.0  
!  
interface Vlan2  
nameif outside  
security-level 0  
ip address dhcp setroute  
!  
interface Ethernet0/0  
switchport access vlan 2  
!  
interface Ethernet0/1  
!  
interface Ethernet0/2  
!  
interface Ethernet0/3  
!  
interface Ethernet0/4  
!  
interface Ethernet0/5  
!  
interface Ethernet0/6  
!  
interface Ethernet0/7  
!  
passwd xxxxxxxxxxxx encrypted  
ftp mode passive  
dns server-group DefaultDNS  
domain-name xxx.xxx  
object-group icmp-type ICMP-INBOUND  
description Permit necessary inbound ICMP traffic  
icmp-object 0  
icmp-object 3  
icmp-object 11  
access-list INBOUND extended permit icmp any any object-group ICMP-INBOUND  
pager lines 24  
logging enable  
logging console notifications  
logging buffered warnings  
logging asdm notifications  
mtu outside 1500  
mtu inside 1500  
icmp unreachable rate-limit 1 burst-size 1
```

PIX 515 - DHCP on WAN - Sample Script

Written by webadmin

Tuesday, 24 May 2011 21:46 - Last Updated Tuesday, 24 May 2011 22:23

```
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group INBOUND in interface outside
timeout xlate 3:00:00
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 uauth 0:05:00 absolute
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd auto_config outside
!
dhcpd address 10.0.0.30-10.0.0.254 inside
dhcpd dns 68.87.64.196 68.87.66.196 interface inside
dhcpd enable inside
!
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
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
```

PIX 515 - DHCP on WAN - Sample Script

Written by webadmin

Tuesday, 24 May 2011 21:46 - Last Updated Tuesday, 24 May 2011 22:23

```
inspect sip
inspect netbios
inspect tftp
!
service-policy global_policy global
webvpn
enable outside
prompt hostname context
```