

## Deploying Secure Guest Networking Environments with NACwalls

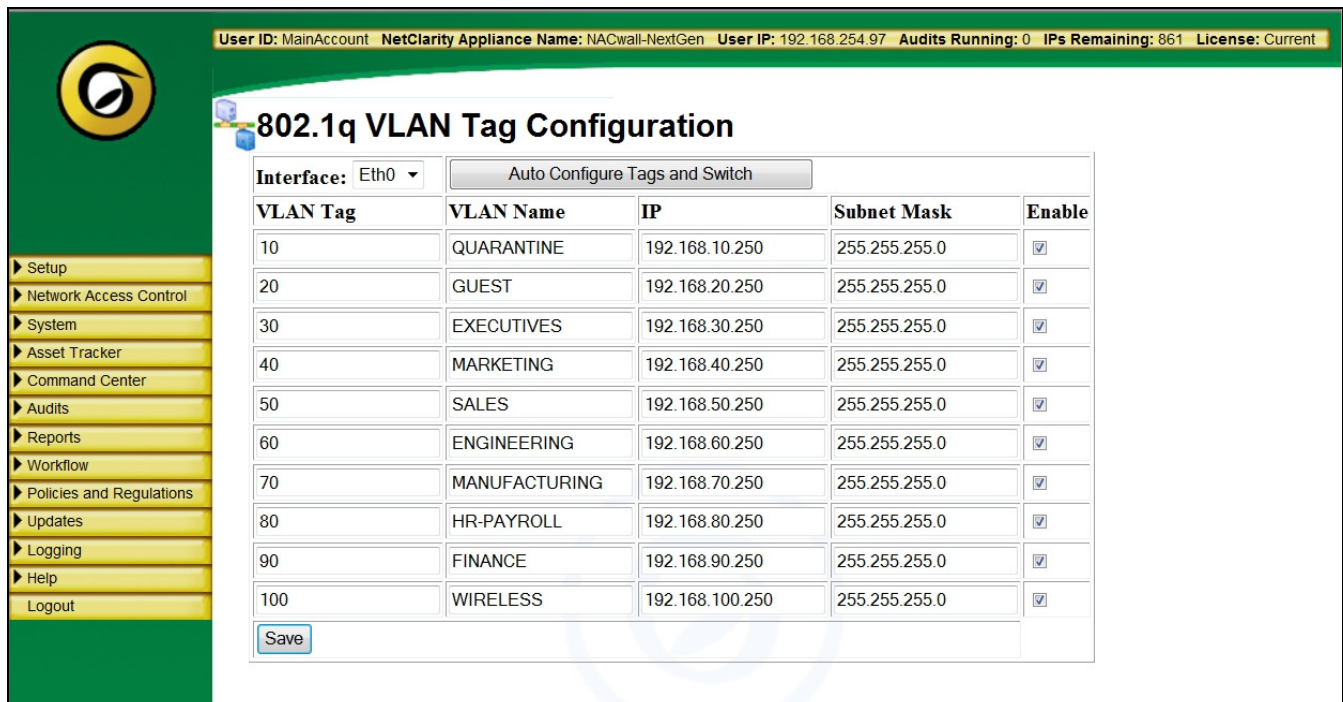
Companies and government organizations including libraries and schools often support guest networks as part of their overall computer networking setup. A guest network is a small section of an organization's computer network designed for use by temporary visitors.

This subnet or virtual local area network (VLAN) often provides full Internet connectivity, but it also strictly limits access to any internal (intranet) Web sites or files.

Besides helping to keep an organization's internal information private, guest networks help avoid spreading any computer worms that visitors may have on their systems. Until NACwalls, setting up and securing a guest network was difficult and cost-prohibitive.

To properly configure a guest network, NetClarity recommends the following network configuration and deployment of the NACwall appliance:

1. Place a low cost managed switch that supports 802.1q (VLAN tagging) on the DMZ port of the corporate or branch office firewall.
2. Take one of the freely available Ethernet ports of the NACwall appliance and plug it into this managed switch.
3. Configure a VLAN called "GUEST" in the NACwall's 802.1q VLAN Tag Configuration screen and map it to the TAG ID of that VLAN on that managed switch.



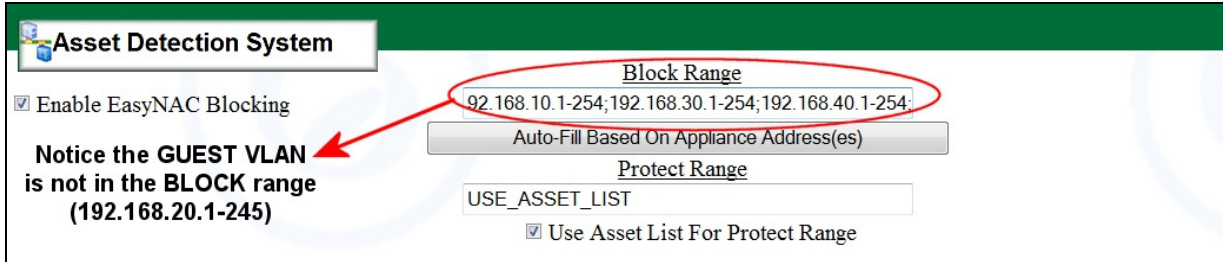
User ID: MainAccount NetClarity Appliance Name: NACwall-NextGen User IP: 192.168.254.97 Audits Running: 0 IPs Remaining: 861 License: Current

### 802.1q VLAN Tag Configuration

Interface: Eth0

VLAN Tag	VLAN Name	IP	Subnet Mask	Enable
10	QUARANTINE	192.168.10.250	255.255.255.0	<input checked="" type="checkbox"/>
20	GUEST	192.168.20.250	255.255.255.0	<input checked="" type="checkbox"/>
30	EXECUTIVES	192.168.30.250	255.255.255.0	<input checked="" type="checkbox"/>
40	MARKETING	192.168.40.250	255.255.255.0	<input checked="" type="checkbox"/>
50	SALES	192.168.50.250	255.255.255.0	<input checked="" type="checkbox"/>
60	ENGINEERING	192.168.60.250	255.255.255.0	<input checked="" type="checkbox"/>
70	MANUFACTURING	192.168.70.250	255.255.255.0	<input checked="" type="checkbox"/>
80	HR-PAYROLL	192.168.80.250	255.255.255.0	<input checked="" type="checkbox"/>
90	FINANCE	192.168.90.250	255.255.255.0	<input checked="" type="checkbox"/>
100	WIRELESS	192.168.100.250	255.255.255.0	<input checked="" type="checkbox"/>

Turn on the Asset Detection System to BLOCK rogue access to the corporate network but EXCLUDE the GUEST VLAN from the BLOCK RANGE. Make sure a valid email is setup to receive alerts.



**Asset Detection System**

Enable EasyNAC Blocking

**Notice the GUEST VLAN is not in the BLOCK range (192.168.20.1-245)**

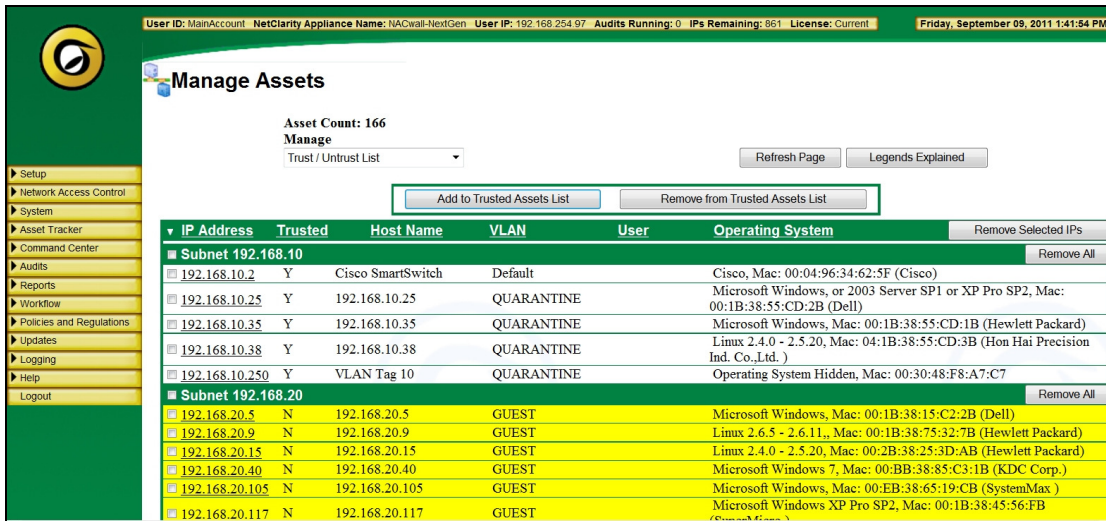
**Block Range**  
 192.168.10.1-254;192.168.30.1-254;192.168.40.1-254

Auto-Fill Based On Appliance Address(es)

**Protect Range**  
 USE\_ASSET\_LIST

Use Asset List For Protect Range

Anytime a guest arrives on that VLAN (which could also be the local SUBNET of a WIRELESS ROUTER plugged into the DMZ port of the firewall instead of a managed switch), they will show up as YELLOW (untrusted but not blocked) in the NACwall Manage Assets user interface and an alert will be sent. As long as they stay on the GUEST VLAN (or the wireless subnet) they will not be quarantined.



User ID: MainAccount NetClarity Appliance Name: NACwall-NextGen User IP: 192.168.254.97 Audits Running: 0 IPs Remaining: 861 License: Current Friday, September 09, 2011 1:41:54 PM

**Manage Assets**

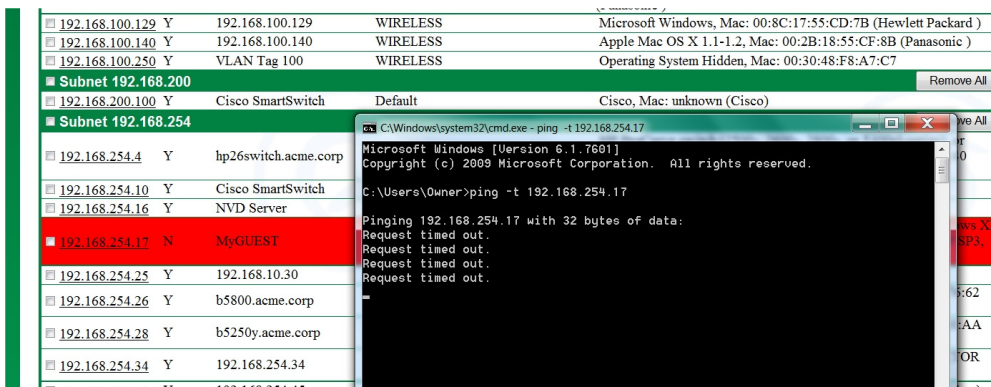
Asset Count: 166  
 Manage  
 Trust / Untrust List

Refresh Page Legends Explained

Add to Trusted Assets List Remove from Trusted Assets List

IP Address	Trusted	Host Name	VLAN	User	Operating System	Remove Selected IPs
<b>Subnet 192.168.10</b>						
192.168.10.2	Y	Cisco SmartSwitch	Default		Cisco, Mac: 00:04:96:34:62:5F (Cisco)	Remove All
192.168.10.25	Y	192.168.10.25	QUARANTINE		Microsoft Windows, or 2003 Server SP1 or XP Pro SP2, Mac: 00:1B:38:55:CD:2B (Dell)	
192.168.10.35	Y	192.168.10.35	QUARANTINE		Microsoft Windows, Mac: 00:1B:38:55:CD:1B (Hewlett Packard)	
192.168.10.38	Y	192.168.10.38	QUARANTINE		Linux 2.4.0 - 2.5.20, Mac: 04:1B:38:55:CD:3B (Hon Hai Precision Ind. Co.,Ltd. )	
192.168.10.250	Y	VLAN Tag 10	QUARANTINE		Operating System Hidden, Mac: 00:30:48:F8:A7:C7	
<b>Subnet 192.168.20</b>						
192.168.20.5	N	192.168.20.5	GUEST		Microsoft Windows, Mac: 00:1B:38:15:C2:2B (Dell)	
192.168.20.9	N	192.168.20.9	GUEST		Linux 2.6.5 - 2.6.11, Mac: 00:1B:38:75:32:7B (Hewlett Packard)	
192.168.20.15	N	192.168.20.15	GUEST		Linux 2.4.0 - 2.5.20, Mac: 00:2B:38:25:3D:AB (Hewlett Packard)	
192.168.20.40	N	192.168.20.40	GUEST		Microsoft Windows 7, Mac: 00:BB:38:85:C3:1B (KDC Corp.)	
192.168.20.105	N	192.168.20.105	GUEST		Microsoft Windows, Mac: 00:EB:38:65:19:CB (SystemMax )	
192.168.20.117	N	192.168.20.117	GUEST		Microsoft Windows XP Pro SP2, Mac: 00:1B:38:45:56:FB	
<b>Subnet 192.168.200</b>						
192.168.200.100	Y	Cisco SmartSwitch	Default		Cisco, Mac: unknown (Cisco)	Remove All
<b>Subnet 192.168.254</b>						
192.168.254.4	Y	hp26switch.acme.corp				
192.168.254.10	Y	Cisco SmartSwitch				
192.168.254.16	Y	NVD Server				
192.168.254.17	N	MyGUEST				
192.168.254.25	Y	192.168.10.30				
192.168.254.26	Y	b5800.acme.corp				
192.168.254.28	Y	b5250y.acme.corp				
192.168.254.34	Y	192.168.254.34				

If they attempt to gain rogue, malicious, internal access to your corporate network they will automatically be BLOCKED and their device will show up on the Manage Assets page on the other VLAN or other subnet marked in RED (untrusted and being blocked).



192.168.100.129	Y	192.168.100.129	WIRELESS		Microsoft Windows, Mac: 00:8C:17:55:CD:7B (Hewlett Packard )
192.168.100.140	Y	192.168.100.140	WIRELESS		Apple Mac OS X 1.1-1.2, Mac: 00:2B:18:55:CF:8B (Panasonic )
192.168.100.250	Y	VLAN Tag 100	WIRELESS		Operating System Hidden, Mac: 00:30:48:F8:A7:C7
<b>Subnet 192.168.200</b>					
192.168.200.100	Y	Cisco SmartSwitch	Default		Cisco, Mac: unknown (Cisco)
<b>Subnet 192.168.254</b>					
192.168.254.4	Y	hp26switch.acme.corp			
192.168.254.10	Y	Cisco SmartSwitch			
192.168.254.16	Y	NVD Server			
192.168.254.17	N	MyGUEST			
192.168.254.25	Y	192.168.10.30			
192.168.254.26	Y	b5800.acme.corp			
192.168.254.28	Y	b5250y.acme.corp			
192.168.254.34	Y	192.168.254.34			

```

C:\Windows\system32\cmd.exe - ping -t 192.168.254.17
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Owner>ping -t 192.168.254.17

Pinging 192.168.254.17 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
  
```

Guest networking made easy.