

Vanguard Applications Ware
Release 7.2 Service Pak 1.0 (7.2S100)
Software Advisory Notice

1) Introduction

This notice contains information on software improvements and changes made by the Vanguard Applications Ware Release Service Pak 7.2S100.

This notice supplements the Vanguard Applications Ware R7.2R00A Software Release Notice (Part Number T0294 Rev D)

Release 7.2.S100 extends the multi-service convergence benefits of enterprise access gateways with the following new features and enhancements. You can also find summaries for these in Section 5 of this document or detailed descriptions of the new Release 7.2S100 features in the referenced documents at the following web site:

<http://www.vanguardnetworks.com/support-documentation-overview.htm>

- MD5 - BGP peer authentication
- Voice Enhancements: SIP Connect 1.0, Fax, On Hold Media Attribute, IP Classifier, Traffic Conditioner & QoS Mapper Profile Configuration, H.323 Caller ID, MoI CDR Enhancements, UAE Radio Half-Duplex
- NHRP (Next Hop Resolution Protocol) registration
- 7300 Platform System Card New Revision – V3
- Null Routes
- Firewall Control-Plane and Firewall Policy Traffic Logging
- IPSEC Aggressive Mode
- PPP/IPCP learned IP address line
- SSH
- TCP Statistics

2) Overview

Products supported by Release 7.2S100

Product	Support
Vanguard 3410, 3460, 3480	Normal Product Release
Vanguard 6840, 6841	Normal Product Release
Vanguard 7310, 7330	Normal Product Release, V3 New Card
Vanguard 242D	Normal Product Release
Vanguard 340 Enhanced	Normal Product Release
Vanguard 342	Normal Product Release

Release 7.2S100 is not supported on these discontinued products:

Product	Last Release Supported
Vanguard 100	Maintained at 5.3M.
Vanguard 200	Maintained at 5.1M.
Vanguard 300	Maintained at 5.4.
Vanguard 305	Maintained at 5.5.
Vanguard 311	Maintained at 5.1M.
Vanguard 31x+	Maintained at 5.3M.
Vanguard 320	Maintained at 6.4.R10A.
Vanguard 6425, 6430, 6450	Maintained at 6.0.R00A.
Vanguard 340	Maintained at 7.0.R00A.
Vanguard 6435, 6455	Maintained at 7.0.R00A.
6500+	Maintained at 5.1M.
650-D	Product maintained at 5.0c. The battery backup version has been sunset.
Vanguard 6520	Product maintained at 5.5
Vanguard 6560	Product maintained at 6.0.R00A

3) Install Service Pack

Executable File

Follow these steps to install the Service Pack 7.2.S100 patch executable file:

Note

For more detailed patch installation instructions, refer to the *Vanguard Software Builder Manual* (Part Number T0030).

Step Action

1. If you have not already done so, install Vanguard Software Builder from any Vanguard Release 7.2.R00A CD-ROM (**Part Number 72608-40 A**).

2. Download the 72S100.ZIP file from Vanguard Networks, please save the file to a local drive on your computer.
http://www.vanguardnetworks.com/support/downloads/service_paks/

3. Use WinZip® to extract the ZIP file. The 72S100.ZIP file contains the 72S100.EXE file.

4. Run or open the 72S100.EXE executable file from your local drive.

5. The patch executable file prompts you with installation instructions. Insert the Vanguard 7.2.R00A CD-ROM into the CD-ROM drive and select its drive letter. Follow the installation instructions provided by the installer.

Part No. 72608-40, Rev A

Build an Image After you install the Service Pack Patch executable file, you must build a custom release and load the custom image.

Note

For detailed instructions on building a software image and using the Vanguard Software Loader, see the *Vanguard Software Builder Manual* (Part Number T0030) and the *Vanguard Software Loader Manual* (Part Number T0057).

Viewing Alarms and Reports

Alarms and Reports appear in the CTP or in your network management system. For explanations of Vanguard alarms and fatal error reports (FERs), see the *Vanguard Alarms and Reports Manual* (Part Number T0005), or visit the Alarms Search database on: www.vanguardnetworks.com/support/

Step Action

1. Using Vanguard Software Builder, build a custom Release 72S100 Service Pak image by selecting the appropriate Release (7.2.S100 for example) from the **Release** drop-down menu. Select features or options that you want to include in the image.

2. Load the custom image using the Vanguard Software Loader.

Part No. 72608-39, Rev A January, 2008

4) Service Pak 7.2.S100 Software Improvements

The table below lists changes request and software improvements. Change request reported to Customer Service have an assigned change request number and in most cases, interim patches are released to fix the problems. These change requests and software improvements are incorporated into the Vanguard Applications Ware Release 7.2.S100 and where applicable, interim patch releases have been replaced by this Service Pak.

Note: The Change Request Number are numbers assigned by Vanguard Networks and are used exclusively for tracking purposes.

<u>Change Request Number</u>	<u>Release Where Problem was Reported or fixed in Patch</u>	<u>Problem Description</u>
16670	6.5.P03E	FXO ports are getting hung and a node boot is required to clear.
17376	70T16F	TCP header compression not working
17509	7.2.P03A	Need to implement more QoS IP CL,Tc Mapper profile entries
17561	7.1.T13A	3 party conference (REFER) is not working
17810	7.2iR00M	PPP/IPCP learned IP addr not shown in IP Interface stats
17851	7.0S100	BGP peer error, BGP - FSM Error - Peer 1 CurrState 0 CurrEvt 2
17869	Feature	Datapac 3201 protocol support on the 3400 platform
17886	70T16Z/Feature	Node freeze after reach 100% CPU. Need CPU reset to recover.
17890	7.2R00A	TOS Stat missing from Cache Statistics
17893	7.1r00a	Out of sequence large pings are failing with ACL, IP.51 rs ovfl alarms
17895	7.2R00A	Domain name field is too short
17904	7.2R00A	Unable to process fragmented ICMP messages when access control is enabled
17909	7.2.R00A	Bypass stations buffer packets during heavy load and stop transmitting
17910	7.2R00A	DHCP Server issues with WIFI networks.
17911	7.2.P01B	arp may set data packet priority to exp_no_drop arputil.c #1091
17923	7.2R00A	Sudden Buffer Depletion when running SIP Voice Loading Test
17927	7.2R00A	Constant Node Crash when T1 ISDN is configured on Int. 1
17930	7.2.R01A	[Node Crash]:Memory Protection: PC stopped at _tcp_close.
17931	7.2.T01B	The rate limit feature was not included in the 342 & 242 platforms
17932	7.2.R01A	[IPSec Aggr Mode]:Node crash due to PPPoE Port configuration
17936	Feature	Add support for Bridge Priority to ethernet switch code
17942	7.1.S100	HTTPD will only accept the last address in an httpd access list
17954	7.2R00A	All IP Sec tunnels go down after booting IPsec parameters, no CTP access
17955	7.2.T02A	Node boot needed to enable ISDN virtual ports once they have been disabled.
17962	7.2P01C	Node will not boot from alternate if current is corrupt.
17965	7.2.P02A	[Hardware Status]:7300s Hardware Status does not reflect the startup diag

17969	7.2.R00A	[ISDN BRI]:x.25 virtual port boot does not work.
17970	7.2.T02A	SNMP MIB does not reflect loss of carrier correctly.
17972	7.2.T02A	SSH password does not work
17986	7.2.P01F	BGP session fails to negotiate
17988	7.2.T02A	[6480]:BRI:Leased bonded 128K link does not work with 6840.
17992	7.2.P02A/Feature	Need TFTP image loading capability in 34xx bootprom
18023	Feature	Implement a half-duplex audio path using E1 CAS signaling
18026	7.2.P01F/Feature	FW/PPoE:Cannot filter traffic destined to the router
18029	7.2	New T1/E1 cards not showing up in power up diagnostics with 3 Serial cards
18032	V7.1.T17A	MLPPP port not recovering after outage using T1 links w remote stand alone DSUs
18033	7.2R00A/Feature	MOI - Requests full support of Voice Billing Enhancements on 6.5T25C & 7.1 PPPoE INITIALIZATION ERROR No ethernet port context alarm after changing config
18034	7.2.T01E	
18040	7.2.P01H	TCP port lock-up prevents remote access to the node - node must be rebooted
18042	NA	BGP hangs intermittently with 2 BGP Peers
18043	7.1P25A	Serial Frame Relay Port has constant CRC errors.
18044	7.1.S100	Qos not marking DSCP at IPsec over Ethernet WAN port
18059	7.2P01H/Feature	SSH is still stranding TCP sessions
18072	7.2.P01K	[Firewall]:No Policy Action Status on Firewall Session Table.
18100	7.2.P01M	[Firewall]:Stats:Wrong Firewall Flow Status with permitted fragmented data
18103	7.2.R00A	PAD port configured for 5 data bits not working, supported?
18118	7.2R00A	BGP is not learning the external networks properly, stats do not show AS
18132	7.2P01P	Node restarts when stressing dual BGP peers with RIP redistribution enabled
18134	7.2.T02C	Fax over G.711 is no longer working
18155	7.2.R00A	BGP is not learning external routes from Backbone properly

5) Overview of Features and Enhancements

MD5 - BGP peer authentication

BGP Peer Authentication is the newest method to reduce security risks in a BGP network. The Vanguard implementation of BGP peer authentication uses the TCP MD-5 signature as specified in RFC 2385. This algorithm takes a key, the password entered during configuration, and performs an MD-5 hash on the key, and sends the resulting hash to the remote peer. The password itself is never sent over the connection.

Both sides of an authenticated BGP peer session must use the same password.

The authentication occurs in the TCP session not on the BGP peer session.

It provides added confidence that packets received from the TCP peer actually originated from the authorized TCP peer.

Though first released in patch 7.2P01D, the following parameter is new and is now generally available in release 7.2S100.

This new parameter “MD5 Password” can be found under “configure>configure router>configure BGP>Peer Parameters”.

MD5 Password

Range	1-25 alphanumeric characters, use the space character to blank field
Default	(blank)
Description	Enter password for TCP MD5 Signature Option. A blank password means the feature is turned off.

Note: SNMP MIB support for this parameter is not available in 7.2S100, that support is forthcoming.

Voice Enhancements: SIP Enhancements

SIP Connect 1.0 Enhancements:

SIPconnect 1.0 is a technical recommendation put out by the SIP Forum that describes the interface between a SIP service provider network and a SIP enterprise network. SIPconnect is the de facto standard for SIP Trunking. The following parameter changes have been made to our product to achieve this functionality.

Change From tag When Authenticating: Disabled/

Range = Disabled,Enabled

Default = Disabled

Disabled - If disabled, authentication requests sent in response to a challenge, which are outside of any dialog, will use the same values for the Call-ID and From tag as in the original request, and the CSeq number will be one higher than in the original request.

Enabled - If enabled, authentication requests sent in response to a challenge, which are outside of any dialog, will use new values for the Call-ID, From tag and CSeq number than those used in the original request.

SIP Signaling DSCP Value: 40/

Range = 0-63

Default = 40

Enter the DSCP value for SIP signaling packets.

SIP RTP DSCP Value: 46/

Range = 0-63

Default = 46

Enter the DSCP value for SIP RTP packets.

On Hold Media Attribute: Sendonly/

Range = Sendonly,Inactive

Default = Sendonly

This parameter specifies the media attribute to use in the SDP when sending an offer to put the remote end on hold.

Sendonly - Specify a=sendonly in SDP.

Inactive - Specify a=inactive in SDP.

Voice Switch Table change in support of SIP E.164 Numbering:

Additional Voice Switching Features: NONE/

Range =NONE,

H323_USE_INTERFACE_IP_ADDR,ENABLE_VOICE_MAIL,E_164_NUMBER

Default = NONE

Select Additional Voice Switching Features

NONE - no features enabled.

H323_USE_INTERFACE_IP_ADDR - Force all outbound H323 calls use the Interface IP address as the Source IP address in H.225, H.245 and media channel connection.

ENABLE_VOICE_MAIL - this switch entry specifies the call address of the voice mail port.

E_164_NUMBER - The digits specified in this entry represent a global E.164 number. The E.164 number syntax will be used in SIP requests.

Any combination of above specified by summing

(e.g. H323_USE_INTERFACE_IP_ADDR+ENABLE_VOICE_MAIL..).

Voice Port Enhancement:

The E&M interface type has been modified to operate slightly different from its original design for Transparent Voice Signaling (TVS) Mode. This parameter is only present when “Signaling Control” is set to Transparent. This new selection will allow the user to enable or disable audio when the signaling bits return to Idle. This is useful for eliminating Echo during some Radio Communication by implementing a forced Half Duplex operation.

Block Audio When Idle: Disabled

Range = Disabled,Enabled

Default = Disabled

This parameter enables/disables the blocking of audio packets toward the interface during the idle signaling state.

Disabled - Audio packets received from remote end will be sent to the interface when the interface is in the idle signaling state.

Enabled - Audio packets received from remote end will be discarded when the interface is in the idle signaling state.

Note: that this parameter must be configured the same at both the local and remote ends of the TVS connection. Otherwise, a one way audio problem could result.

Fax Support Enhancement:

The new T38_Override selection is introduced for those customers who choose to take advantage of the bandwidth savings of T.38 fax operation even when running G.711. Previous operation was for the voice port to stay running G.711 coder even if fax data was detected.

FAX Support:

Range = Disabled,Proprietary,Enabled,T38,T38_Override

Default = Proprietary

This parameter selects whether the FAX data is to be supported.

Proprietary - Detects presence of FAX data. If FAX data is detected, the voice port will spoof the local FAX machine and transmit the Proprietary FAX data to the remote end as 4800bps or 9600bps data.

T38 - Detects presence of FAX data. If FAX data is detected and the current codec is not G.711, the voice port will spoof the local FAX machine and transmit the T.38 standards based FAX data to the remote end. T.38 support fax data rates of 14.4kbps, 12.0kbps, 9.6kbps, 7.2kbps, 4.8kbps or 2.4kbps. If the current codec is G.711, the fax data will be transmitted transparently over G.711.

T38_Override - Detects presence of FAX data. If FAX data is detected,

regardless of the current codec, the voice port will spoof the local FAX machine and transmit the T.38 standards based FAX data to the remote end. T.38 support fax data rates of 14.4kbps, 12.0kbps, 9.6kbps, 7.2kbps, 4.8kbps or 2.4kbps.

Disabled - FAX data will not be detected.

Enabled - Supported for backward compability, equivalent to Proprietary.

Note:

T.38 Fax Requires release 6.3 or greater software, and is available by purchasing a software license. T.38 Fax text is not present if the T.38 Fax option is not loaded. Release 6.4 and greater includes the Fax feature in the Voice Applications Ware License for the Vanguard 34x, 6435 and 6455. The Vanguard 7300 includes the fax feature in the Multi-Service Applications Ware.

Note: T38, T38_Override or Disabled must be selected for DSP Option 4.

Note: T38 and T38_Override cannot be selected for DSP option 1.

IP Classifier, Traffic Conditioner & QoS Mapper Profile Configuration:

This parameter range has been extended from its original range of 1-30 to 1-100.

Entry Number: 1/?

Range = 1-100

Default = 1

Entry number used to reference this table record.

NHRP (Next Hop Resolution Protocol) registration

Vanguard Networks Routers now support NHRP (Next Hop Resolution Protocol).

This was introduced in response to the demand for Vanguard Network routers to operate in the DMVPN (Dynamic Multipoint Virtual Private Network) model.

In the DMVPN model NHRP was required to address the burden of the HUB router in managing its remotes, primarily in the hubs requirement to add configuration for each of the remotes in the network. Using NHRP the Hub no longer has the need to modify/add to the configuration for any remotes added to the network.

The VG first release of NHRP support includes the following;

- Act as Spokes in the Hub & Spoke network
- Use GRE to transport data to the Hub (GRE only)
- Support dynamic IP addressing on the WAN interface.

The First release of Vanguard Networks NHRP implementation does NOT require the Vanguard routers to:

- Act as Hubs
- Be an NHRP Server
- Support direct Spoke-to-Spoke tunnels
- Support dynamic caching of mappings.

The Spokes will always have a static NHRP mapping for the Hub. The Hub must have a static IP address that is known by the Spokes.

Note: SNMP MIB support for NHRP is not available in release 7.2S100, this support is forthcoming.

GRE enhancements in support of NHRP

In support of the NHRP implementation an optional GRE Key (Tunnel Key) is needed to provide a way for the hub routers to map incoming GRE packets to specific tunnel interfaces. Each tunnel interface on a router must have a distinct GRE Key. All tunnels in a given DMVPN must have the same key.

NHRP is configured in the Tunnel configuration found from the main menu under;
 Configuration>Configure Router>Configure Tunnel

The new parameters added to 7.2S100 are;

- * Tunnel Key
- * NHRP Network ID
- * NHS Address
- * NHRP Authentication
- * NHRP Holding Time
- * NHRP Registration Timeout
- * Set NHRP Unique Flag

Here the new parameters are presented with the configurable ranges and brief description as they will appear in the Vanguard Routers Configuration menu.

Tunnel Key

Range	0-4294967295
Default	0
Description	This parameter enables the use of the optional Key field in the GRE header. A value of 0 indicates the GRE Key is not

	used.
--	-------

NHRP Network ID

Range	0-4294967295
Default	0
Description	This is an identifier for a specific NHRP network. Each NHRP network must have a unique Network ID. All nodes in the network must have the same Network ID. A value of 0 indicates the Network ID is not used.

NHS Address

Range	A valid IP address in dotted notation.
Default	0.0.0.0
Description	This parameter specifies the address of the Next Hop Server (NHS). The router will register with the NHS.

NHRP Authentication

Range	0-8 alphanumeric characters, use the space character to blank field
Default	(blank)
Description	This parameter specifies the authentication string used in NHRP messages. If blank, authentication is not used.

NHRP Holding Time

Range	0-65535
Default	7200
Description	This parameter specifies the holding time value in NHRP registration requests. The NHS will cache the registration request for the duration of the holding time value in seconds.

NHRP Registration Timeout

Range	0-65535
Default	2400
Description	Registration requests are sent out every [this parameter] seconds. If this parameter is set to 0, then registration requests are sent out every [1/3of holding time] seconds.

Set NHRP Unique Flag

Range	Yes,No
Default	Yes
Description	This determines whether to set the unique flag in

	registration requests. If the flag is set, the hub will prevent the mapping entry from being overwritten by a registration request with the same protocol address but with a different NBMA address. It's recommended to set this parameter to Yes if the tunnel's source address is static, to No if dynamic.
--	--

Statistics

Statistics supporting NHRP can be found from the main menu under;
 Statistics>Router Stats> Tunnel Stats

Shown here is a sample of the menu followed by samples of the statistics themselves.

Menu: Tunnel Statistics Path: (Main.5.16.11)

1. General Tunnel Statistics
2. Tunnel RTP/UDP/IP Compression Statistics
3. **NHS Statistics**
4. **NHRP Mapping**
5. **NHRP Traffic**

NHS Statistics

Node: vgnhrp1 Address: 100 Date: 16-AUG-2000 Time: 18:59:13
 NHS Statistics

NHS Addr	Reg Req (retry in)	Reg Repl	State	Last Reg Repl
----------	--------------------	----------	-------	---------------

Tnl 1:				
172.020.001.001	536 (NA)	527	Up	16-AUG-2000 18:41:02

NHRP Mapping

Node: vgnhrp1 Address: 100 Date: 16-AUG-2000 Time: 18:59:21
 NHRP Mapping

Iface	Proto Addr	NBMA Addr	Expiry	Type
Tnl 1	172.20.001.001	172.028.124.001	Never	Static

NHRP Traffic

Node: vgnhrp1 Address: 100 Date: 16-AUG-2000 Time: 18:59:26
NHRP Traffic

Sent via Tnl 1:
Req Req 536, Err Ind 0
Received via Tnl 1:
Reg Reply 527, Err Ind 0, Unsupported 0

7300 Platform System Card New Revision – V3

The 7300 system card (IBM750FX) has been revised.

The part number of the 7300 IBM750FX processor card is 76361G01, this can be found on the card itself and also in “Node Statistics” page 5, sample below.

System Controller: Number of ports: 3 Status: Installed and functional
Assembly: 76361G01 V3 Version: D Serial Number: 160064574

Previous revision is Revision B (76361G01)
The latest revision is Revision D (76361G01)

The minimum Software revision to support the New Rev D System Controller Card (Product Code 1112-10037) is now 7.2S100

Note:

Using any previous software release will still allow full functionality of the Rev “D” System card, with the following exceptions:

- The date and time will not be updated correctly.
- Power up Diagnostics will show failures in the two areas shown below, both of which are related to the revision changes.
Testing NVRAM >>-FAILED-<<
0 0 NVRM 0000 0000 0000 0000 0000
- Testing Real Time Clock >>-FAILED-<<

Null Routes

Overview

A Null route is a static route that discards packets. It is used to engineer networks to prevent the use of the default route when the preferred route is lost. In many cases, when a preferred dynamic route is lost, the default route would cause routing loops if used.

A Null Route differs from an IP Filter in that it can be installed and removed from the routing table when its metrics are compared to other routes for the same subnet. IP filters, on the other hand are always in the table.

In 7.2.S100 the nexthop IP address for a static route can be configured as 255.255.255.255. This nexthop will drop packets. A Null route can be used to backup a route from a dynamic routing protocol to prevent routing loops.

Behavior

The default route is configured as a static route with a nexthop to discard the packet. It is configured to be less preferred than the dynamic route protects. Vanguard refers to this as a backup static route.

The Null route behavior differs in some ways from a backup static route.

The Null Route is not advertised. The Null route is not redistributed into another routing protocol.

From a dynamic routing protocol point of view (RIP, RIPv2, OSPF, BGP) a Null route is considered to be no route. That means, when a null route is installed in the routing table, the dynamic routing protocol will issue a WITHDRAW of the route to its neighbors.

A Subnet Route which has only a NULL route as a member of its summary range should not be advertised. If it has been previously advertised by a dynamic routing protocol, it should be withdrawn.

Configuration Requirements:

To activate the Null Routes feature, Override Static Routes in Configure IP Interface configuration Table must be enabled.

Then, configure Next Hop in Static Routes Configuration as 255.255.255.255 with a bigger number of Metric compared to other routes for the same subnet IP.

[1] Next Hop: 0.0.0.0/?

Range = A valid IP address in dotted notation

Default = 0.0.0.0

The IP address of the next hop to the destination. The next hop itself must be on an IP network directly connected to the router. If the next hop is an unnumbered interface, enter 0.0.0.N where N is the (interface number - 1). If next hop is 255.255.255.255, the route is a null route.

Firewall Control-Plane and Firewall Policy Traffic Logging

Overview

Firewall Control-Plane policies control traffic destined to the firewall in the same way general firewall policies control traffic between zones across the firewall. These policies provide finer control to traffic terminating at the router itself.

Firewall policies will have an option to log traffic matching the firewall policy. These entries are recorded in the new Traffic Log.

Firewall Control-Plane Policies

Firewall control plane policies are used to filter traffic terminating at the router itself. A separate set of policies is advantageous for several reasons. In many cases traffic may not need filtering through the router. In these cases, subjecting all packets to the policies is known to significantly increase the CPU utilization. By separating the policy control for traffic to the router into a separate set, it also makes the intent of the configuration much clearer.

In Configure Firewall Policies, Trust -> Control-Plane, Untrust -> Control-Plane, and DMZ -> Control-Plane are added as follows:

Node: Node3463 Address: 3463 Date: 24-JUN-2010 Time: 13:56:17

Menu: Configure Firewall Policies Path: (Main.6.15.6.2)

1. Trust->Untrust
2. Untrust->Trust
3. Trust->DMZ
4. DMZ->Trust
5. DMZ->Untrust
6. Untrust->DMZ
7. Trust->Control-Plane
8. Untrust->Control-Plane
9. DMZ->Control-Plane

Firewall Policy Traffic Logging

Each firewall policy has a configurable parameter, Traffic Logging, to enable or disable logging for packets matching that policy. The default policy (implicit deny, if no policies match) has no logging. To log a “catch-all” deny, an explicit policy must be configured.

[1] Traffic Logging: None/?

Range = None,Start,End

Default = None

This parameter controls the logging of events to the Firewall Traffic Log and to Syslog, if Syslog is enabled.

None - Logging is disabled.

Start - An event is logged when a flow matching this policy is created.

End - An event is logged when a flow matching this policy closes.

Close events reflect the statistics for the entire session.

Specify a combination by summing individual values

(ex: Start+End)

The traffic logging messages contain:

- Year-Month-Day
- Time (to the second)
- Action (Permit or Deny)
- Ingress Zone
- Egress Zone
- Policy Entry Number
- Source Address
- Destination Address
- Protocol
- Source Port number (if applicable)
- Destination Port number (if applicable)
- Reason

Traffic Log Statistics

The traffic log is kept in memory as a separate log for viewing by the operator. For ease of searching, it shall be kept as an array of traffic log data structures. The array size should be 4K entries.

An entry will be added under the existing Firewall Stats menu, "Firewall Traffic Log". Select "Firewall Traffic Log" to view the current entries in the traffic log.

Node: root Address: (blank) Date: 21-NOV-2000 Time: 22:48:47

Menu: Firewall Stats Path: (Main.5.16.6)

1. Firewall Policy Stats
2. Firewall Traffic Log

#Enter Selection: 2

Node: root Address: (blank) Date: 21-NOV-2000 Time: 22:48:47

Firewall Traffic Log

Page: 1

```
start_time="2003-04-19 02:00:55" ingress_zone=DMZ egress_zone=Control-Plane poli
cy_num=2 policy_action=Permit src=172.16.1.57 dst=150.30.1.74 proto=1 icmp_type=
8 icmp_code=512 reason=Creation
```

IPSec Aggressive Mode

Overview

When the Juniper SSG router is configured to accept VPNs from peers with unknown IP addresses, they requires the ISAKMP Phase 1 negotiation to be in Aggressive mode and have a Peer ID to identify the remote peer.

Vanguard implemented Aggressive Mode with the ability to specify a Peer identifier for compatibility with the Juniper SSG family.

[1] ISAKMP Phase 1 Exchange Type: MAIN_MODE/AGRESSIVE_MODE/?

Range = MAIN_MODE,AGRESSIVE_MODE

Default = MAIN_MODE

ISAKMP Phase 1 exchange type:

Main Mode - More secure option; generally preferred.

Aggressive Mode - Less secure option. Used with dynamic local addressing
it is necessary for interoperability with some VPN concentrators.

[1] ISAKMP Username ID: (blank)/?

Range = 1-63 alphanumeric characters, use the space character to blank field

Default = (blank)

ISAKMP ID payload identifier. This parameter is required, when configured for 'Aggressive' Phase I key change mode. Both U-FQDN and FQDN are supported.

PPP/PCP learned IP address line

PPP/PCP address negotiation

When an interface is configured as unnumbered and the PPP Profile will negotiation and accept its address from its peer, the address will be installed in the router interface.

Note that the subnet mask used will be the one configured by the user. If the router interface as a user configured IP address, PPP/PCP will not install an IP address even if the address negotiated is different than the one configured by the user.

SSH

The SSH configuration parameters now include an idle timeout feature. The default timeout is 15 minutes. SSH statistics now include SSH session statistics that show the current state of the SSH sessions, the username logged into the session, the authentication method, and the IP address and port the user logged in from.

TCP Statistics

TCP statistics now include both a summary statistics menu entry and a detailed statistics

entry. The summary statistics table displays counts for current TCP server-side sessions. The detailed statistics provide more information on each TCP session. Detailed statistics can be searched by server-side TCP port number. If the default port number 0 (zero) is used, all sessions will be displayed.

6) Known Software Limitations

1) CR17945 - For PAD Port Auto Baud Sequence DOT_DOT_CR, two or three "."s are accepted prior to the "CR". More than three "."s prior to the "CR" is not acceptable and may result in the Auto Baud Sequence to resynchronize and restart its search, for the DOT_DOT_CR sequence.

Workaround:

The DTE Device connected to the PAD Port must ensure that it transmits two or three "."s, and does not attempt to transmit more than three "."s prior to the "CR".

2) CR17916 - Invalid RFC1294 encapsulation errors when running an LCON, with RTP/UDP Header Compression, between Releases 6.5R00A and 7.0R00A or greater.

Work Around:

Users must disable RTP/UDP Header Compression.

3) CR16844 -GRE Tunnels may activate ISDN

Encryption session keep-alives trigger GRE tunnels and ISDN calls even when there is no data to be sent.

Workaround: Increasing the session timeout in the encryption profile will decrease the frequency of the extra ISDN calls.

4) CR16941 - Only the first 155 entries in the Virtual Port Mapping Table are valid.

The available range in the VPMT is 1-255. If you use entries above 155 the mapped Voice port will become disabled.

Workaround: Limit configuration to the first 155 VPMT table entries.

5) CR17539 BRI: Interface remains "IDLE" after the node is booted.

If the node is booted while an ISDN call is active, the Interface may not recover and continue to pass data.

Workaround: After booting the interface, Boot Virtual Port Boot. If unsuccessful, unplug and plug the cable back in.

6) CR17579/17354 - Changing the Master Voice Port DSP Image Selection and Booting the Voice Port causes the DSP to reset.

When the master voice port DSP Image selection is changed and the port is booted, the DSP associated with the Voice Port will reset requiring a Node Boot.

Work Around: Boot the node when modifying the DSP image selection.

7) CR17595 - ISDN calls may be initiated with no data incoming.

The node brings up ISDN calls after the previous connections were disconnected even when no data was incoming. It is caused by an inappropriate value configured in Idle Disconnect Timer.

Workaround: Configure the Idle Disconnect timer to be at least 3 times as big as

Add/Remove

Bandwidth Wait Time.

Here are configuration samples:

The following configuration works:

Add Bandwidth Wait Time: 10

Remove Bandwidth Wait Time: 10

Idle Disconnect Timer: 30

Proprietary Page 14 12/4/2009

Vanguard Networks Applications Ware Software Release R7.2R00A Part No. T0294, Rev. D
Dec 2009

But this second example does not work:

Add Bandwidth Wait Time: 10

Remove Bandwidth Wait Time: 10

Idle Disconnect Timer: 25

8) CR17872 - Incorrect Vanguide Builder Error Message when exceeding available flash size of the 34X.

In Vanguide Software Builder selecting Products 340E, 342 or 242d, you may receive the following splash messages if the "Selected Option Size" (estimated calculation) exceeds 8,000,000 due to the image size exceeding the on board flash device limitation.

The on-screen message seen is as follows:

ERROR: No XRC file has been created in the TEMP directory!

Failed to create an XRC file! Please verify correctness of the settings in the "Settings" dialog. Also ensure that there is at least 30MB available on your hard disk and that available Virtual Memory is a least 16MB.

You should now review and save to a different location the .LOG files from the installation's TEMP directory. Do you want to review and save the error logs?

Workaround: Deselect Feature/Protocols until the "Selected Option Size" is below 8,000,000. Note that this calculation will be corrected in the next release of Vanguide Software Builder.

9) CR17677 - IP Parameter Boot may result in a BGP session boot.

Any changes made to BGP related parameters under IP parameters and an IP parameter boot is performed, all BGP sessions will also be booted (reset). This will interrupt live BGP peer sessions and result in network BGP resynchronization.

Workaround: Users should be aware that if a change is made to any of these parameters and a subsequent "IP parameter" boot is performed then all BGP peer sessions will reset to implement the change.

BGP to RIP Enable: Disabled/

BGP to RIP Default Filter: Deny/

BGP to RIP Nondefault Route Override: Disable/

BGP to RIP Default Route Override: Disable/

BGP to RIP Default Metric: 1/

To minimize the impact on the user, perform the IP parameter boot during a scheduled maintenance window to avoid network disruptions. There is no plan to correct this issue.

10) CR18164 - Bridging (total = 1)

Vanguard products support bridging of data traffic for Token Ring and Ethernet LANs.

Bridging LAN traffic minimizes your networking costs by eliminating the need for redundant networks and maximizes the availability of dedicated facilities such as servers and printers, as well as public Frame Relay and X.25 services, across multiple LANs.

Note:

Vanguard 3480 Switch does not support the Bridging feature.

11) CR17762 - Problem Description:

On the VN3480, when two Ethernet Ports (24 through 27) are configured with their Switch Capabilities set to SWITCH_TO_ROUTER_UPLINK and their associated the Router Interface has the same VLAN ID setting and the same subnet IP Address, the higher numbered port will have a Port Status of "MISCONFIG", when the router is Warm Booted.

Work Around:

It is recommended that when more than one VN3480 Ethernet Port (24 through 27) is configured with a Switch Capabilities of SWITCH_TO_ROUTER_UPLINK, their associated Router Interfaces should be configured with a unique VLAN ID and with a unique IP Address.

For example, this is a valid configuration:

Port 24:

[24] *Switch Capabilities: SWITCH_TO_ROUTER_UPLINK

[24] *Router Interface Number: 2

Port 26:

[26] *Switch Capabilities: SWITCH_TO_ROUTER_UPLINK

[26] *Router Interface Number: 4

IP Interface Configurations:

Entry Number:2

[2] Interface Number: 2

[2] IP Address : 192.168.3.1

[2] VLAN ID: 1

Entry Number:4

[3] Interface Number: 4

[3] IP Address : 150.30.1.1

[3] VLAN ID: 2

This is an invalid configuration:

Port 24:

[24] *Switch Capabilities: SWITCH_TO_ROUTER_UPLINK

[24] *Router Interface Number: 2

Port 26:

[26] *Switch Capabilities: SWITCH_TO_ROUTER_UPLINK

[26] *Router Interface Number: 4

IP Interface Configurations:

Entry Number:2

[2] Interface Number: 2

[2] IP Address : 192.168.3.1

[2] VLAN ID: 1

Entry Number:4

[3] Interface Number: 4

[3] IP Address : 150.30.1.1

[3] VLAN ID: 1

12) CR18011 - BGP Load balancing produces an imbalanced ratio

In certain cases traffic flows are not evenly distributed across equal cost links. If one link is an Ethernet port and the other is a PPP serial link, load balancing may skew over time. If both links are either Ethernet or PPP load balancing works properly.

Workaround: Enable firewall. Put all interfaces in the Trust Zone. Enable intrazone routing.