

Application Note

Next Generation Extended Enterprise

IVE, Routing, Firewall, IDP, and Application Acceleration

Kelly Brazil

Alan Sardella



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 350069-001 July 2005

Contents

Contents	2
Executive Summary	3
Overview of Secure Access with IDP, Firewall, SLB and Optimization	3
About the IVE 5.0 Release	4
Secure Access Platform with IDP and/or Firewall	4
IDP with SA	4
SA with Both IDP and Firewall	6
Secure Access Solution with DX	7
Application Front End	8
Load Balancing	9
High Availability	9
HA for IVE	9
HA for IDP	10
HA for DX	11
Network Diagram	11
Configuration of the Solution	11
Router and Firewall	11
IVE	12
IDP in Transparent Mode	18
DX Load Balancing (DX-A)	21
Use of Half-NAT	21
Connectivity to the VIP	21
SLB Groups	21
DX Application Acceleration (DX-B)	22
Conclusion	23
Appendix A: Sizing a Deployment	23
Appendix B: Configurations	24
Edge Router	24
Firewall	24
DX - A (Load Balancing)	25
IVE (Secure Access 3000)	30
IDP	30
DX - B (Application Acceleration)	30

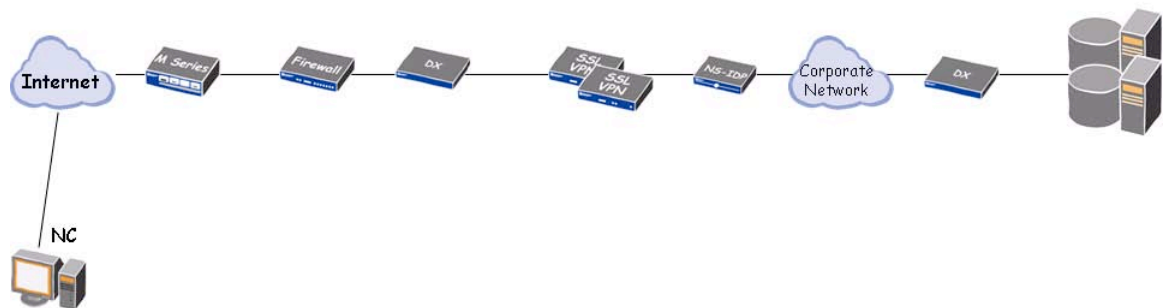
Executive Summary

This application note describes a network built in a Juniper sales lab to illustrate a remote access solution for an extended enterprise. The solution includes the high performance and easily-maintainable Secure Access architecture, configured in high availability mode and load balanced by the DX application accelerator. It also includes the Juniper Networks Intrusion Detection and Prevention (IDP) platform, and a second DX to optimize user sessions and accelerate applications. All of the devices shown in this application note can be configured in high availability mode, although for simplicity high availability mode is not shown in all cases.

As competing forces push businesses to improve productivity by delivering application and information resources to employees, partners, and customers, a new level of control is needed for remote access to these resources in the extended enterprise. Juniper Networks provides the leading remote access solutions on the market today, in terms of capacity, performance, high availability, and ease of management. As the market leader in remote access solutions for the extended enterprise, Juniper provides tested solutions for deployment over any IP infrastructure. The network described herein is one such solution.

This application note discusses some common considerations with Juniper Networks' secure access solution. A sample network (Figure 1) that illustrates a representative solution for an extended enterprise solution is introduced, and configuration tips are presented. Finally, the appendixes of this document provide detailed, annotated full configuration of this network to assist in the building of a similar network for production use.

Figure 1: Complete Extended Enterprise Solution



This complete extended enterprise solution includes Routing, Firewall, Load Balancing, Instant Virtual Extranet, IDP, and Application Acceleration. Remote users of all types (partners, customers, employees) can access the enterprise data center with high performance and high security.

Overview of Secure Access with IDP, Firewall, SLB and Optimization

The enterprise user base includes employees, business partners, and customers, connecting from many different locations with many different devices. The Juniper Networks Instant Virtual Extranet (IVE) platform provides the following access options: core (web-based),

Secure Application Manager (SAM) which is a client/server option, and Network Connect (NC), which is full LAN access. Of course, the most flexible and powerful option is NC. IVE 5.0 greatly enhances the performance of NC; this is discussed in the following section.

About the IVE 5.0 Release

With the IVE 5.0 release, the enhanced SSL VPN solution serves as a single access platform for the extended enterprise. IVE 5.0 delivers the next generation of Network Connect and advanced endpoint remediation capabilities; the new software also offers dynamic XML re-writing and a Java Applet Delivery Infrastructure.

With IVE 5.0, enterprises can deploy one platform to easily and securely meet the diverse access needs of users, from Web applications to streaming media or VoIP apps. The NC 5.0 option has a dual mode option for a unique combination of high performance and high availability. This option combines the best of SSL and IPSec, so that the default connection is via IPSec (which will be higher performing), and if that connection is lost then it fails over to SSL for a high availability option.

IVE 5.0 is the most comprehensive application and network access methods to enable enterprises to leverage one single infrastructure for all their extended access needs. With IVE 5.0, a single platform provides intelligent access provisioning and coordinated security policy administration.

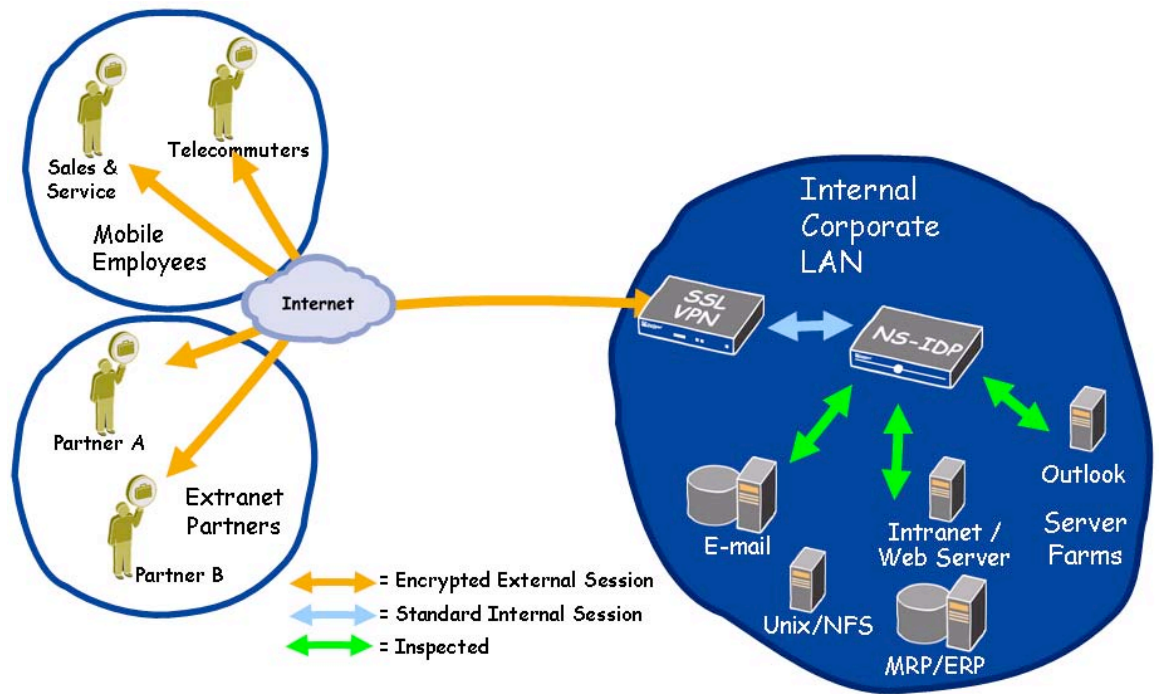
Secure Access Platform with IDP and/or Firewall

Figure 2 shows the addition of IDP to a Secure Access (SA) network. Remote access networks are a common vector for introducing worms and viruses into the corporate LAN. An IDP solution is highly recommended to protect the internal network from full Layer 3 remote access clients, such as traditional IPSec and NC users. In addition to this, the IVE provides unparalleled host checking capabilities that can be used in conjunction with an IDP solution to further protect the corporate LAN. For more information about client-side host checking see the *J.E.D.I. Solution Guide* at www.juniper.net.

IDP with SA

The IDP could be sized to just look at the output of the SSL VPN or it could be placed in front of the server farm, or both.

Figure 2: The Secure Access Network Platform with IDP

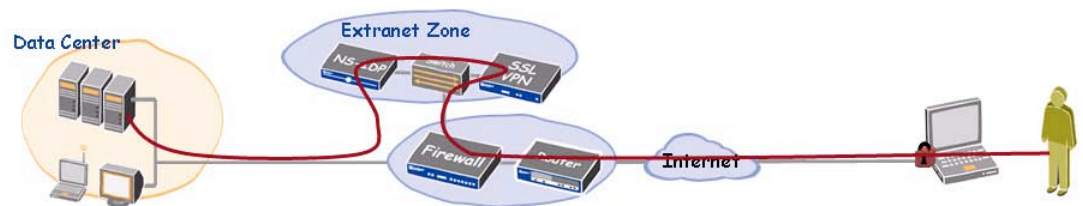


The scaling of the IDP into the network can be based on several factors, such as:

- (1) Does the client want to protect the servers just from the SA data or
- (2) To protect all of the servers or
- (3) Both of the above using multiple segments on one or more boxes.

The IDP can be set directly behind the SSL VPN in the perimeter. When this is done, all Network Connect user traffic will pass through the IDP. Alternatively, all traffic can pass through the IDP. These options are shown in the following figures.

Figure 3: IDP Directly Behind SSL VPN in Perimeter

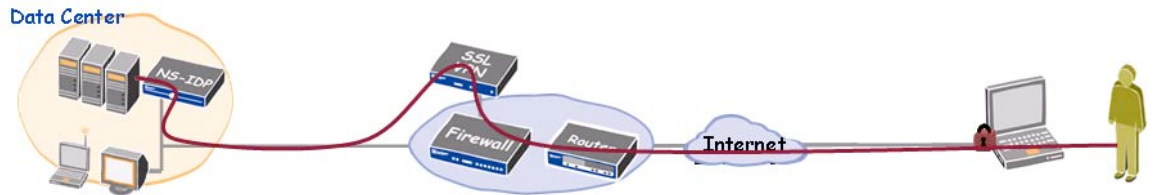


When IDP is set directly behind the SSL VPN in the perimeter, all NC traffic passes through the IDP. If some users are using access options other than core, all traffic will pass through the IDP, but IDP has the most value for the NC traffic. (Core access traffic is only accessing Web

applications, and SAM traffic can be used for client/server access, but NC traffic can access the entire LAN.)

The other option is to have IDP in front of the servers, in the data center.

Figure 4: IDP In Front of Servers



With this option, the IDP is inspecting all traffic accessing the data center, including internal user traffic. This will necessitate greater IDP capacity.

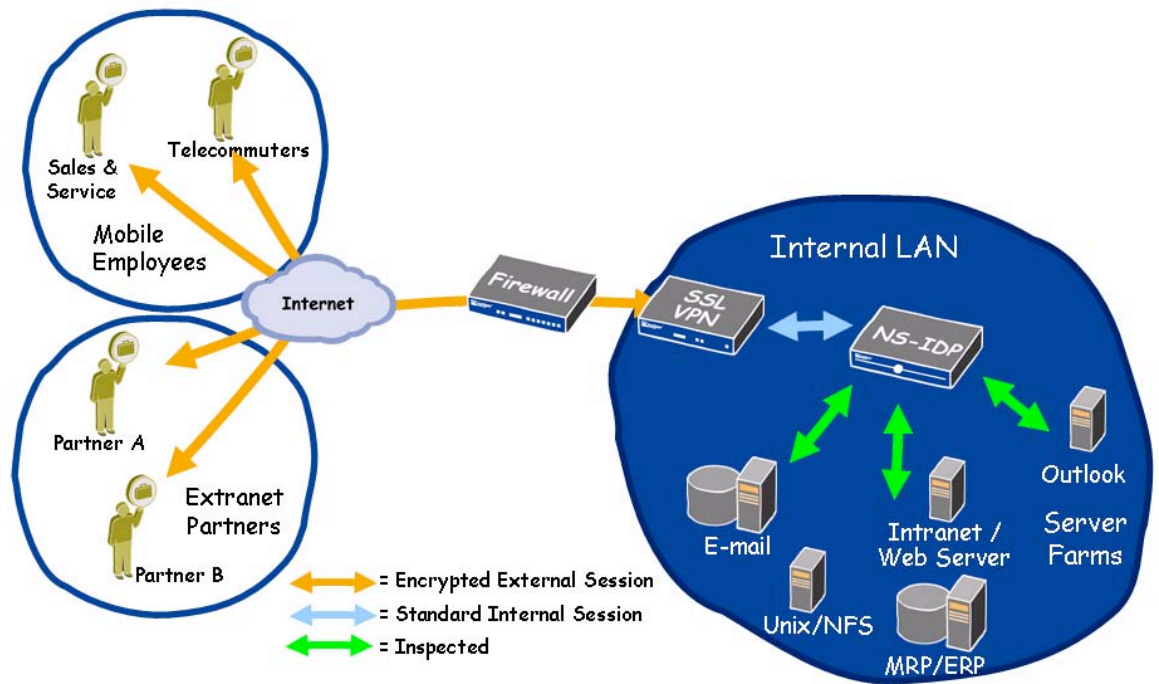
SA with Both IDP and Firewall

The SA platform can be combined with both IDP and the firewall.

Most enterprises want standard outgoing access for the internal host and other functions. Changes in the extranet could potentially mean needing to upgrade the firewall.

The Firewall could be needed for coarse-grained security work. For instance, a policy could be set for any host to access the SA using port 443, or IPSec with UDP port 4500; all other connection attempts can be denied. For usability, it is typically recommended to allow Port 80 to the IVE for usability. Alternatively, the SA can access the internal trust network with no rules.

Figure 5: SA Platform with IDP and Firewall



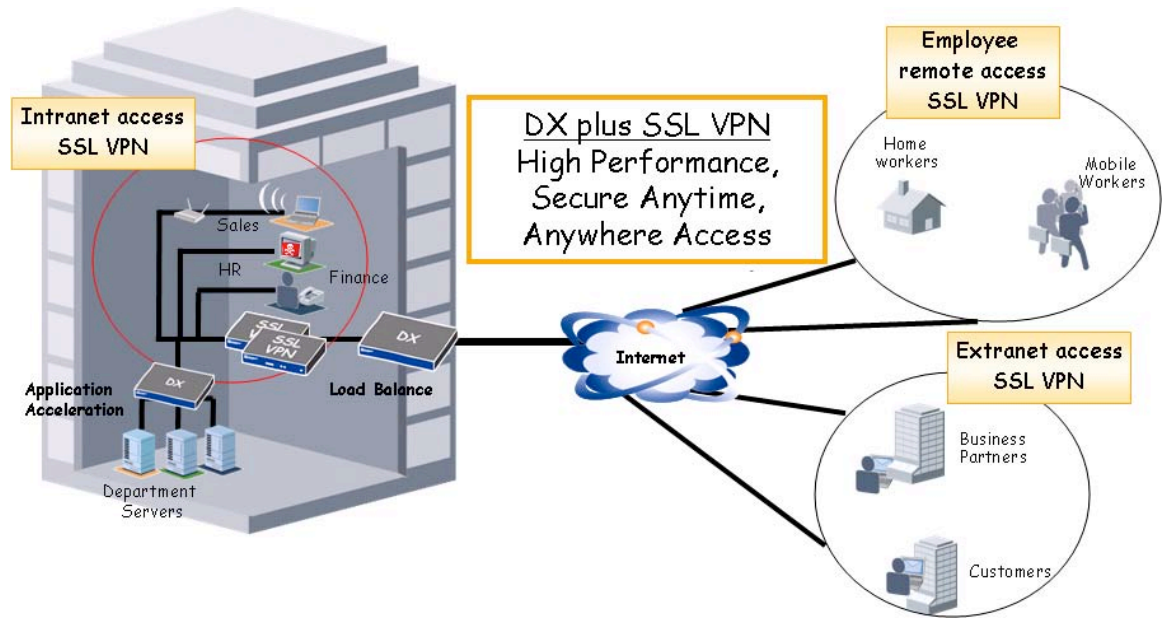
The IDP is best placed just after the SA, so that it can inspect a standard internal session. That way, the traffic is inspected before it reaches the servers.

Secure Access Solution with DX

The Juniper Networks DX application acceleration platform is an application front end (AFE). The DX manages all connections and requests between servers and users, thus maximizing available server and network resources, freeing web server CPUs for other tasks. The DX series also provides full Layer 4-7 load balancing.

The following figure illustrates the use of DX as both a load balancer and application accelerator.

Figure 6: DX and SSL/VPN in the Enterprise

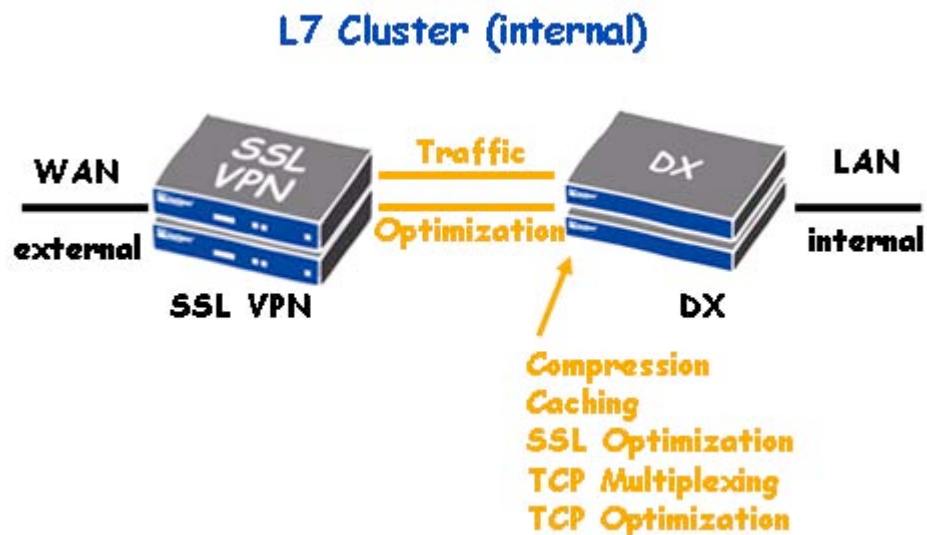


Both uses of the DX are illustrated in this application note.

Application Front End

The DX can be used to accelerate application servers whether the server farm is internal or external. In this application note, an internal server farm is assumed.

Figure 7: DX Front Ending Application Servers (Internal)



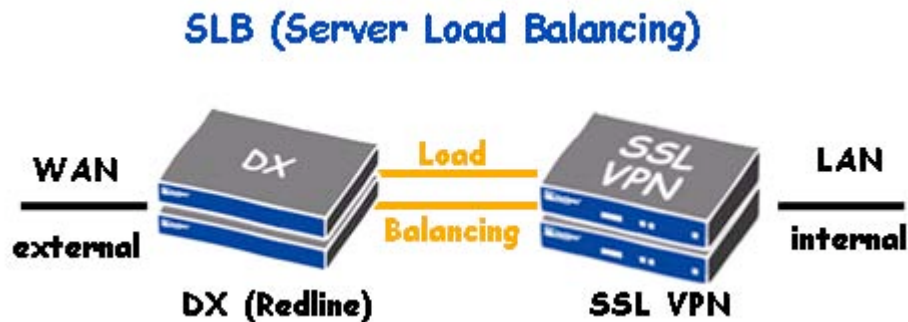
This configuration provides backend application server load-balancing, and TCP

optimization, as well as SSL and TCP offloading. It reduces the response time of web-based applications, particularly when accessed over the extended LAN and via the SAM or NC access methods. It also provides compression and caching, and TCP multiplexing and optimization.

Load Balancing

The DX is also used in this scenario for load balancing of the SA-3000 devices.

Figure 8: DX for Server Load Balancing (External)



This is an excellent solution for Active/Active SSL VPN clustering deployments. Providing Layer 4 load balancing with multi-unit HA support, it supports all SSL VPN access methods (CORE, SAM, and NC) and benefits any SSL VPN appliance model.

High Availability

All Juniper Networks enterprise network elements have high availability (HA) options; options for IVE, IDP and DX are discussed here.¹

HA for IVE

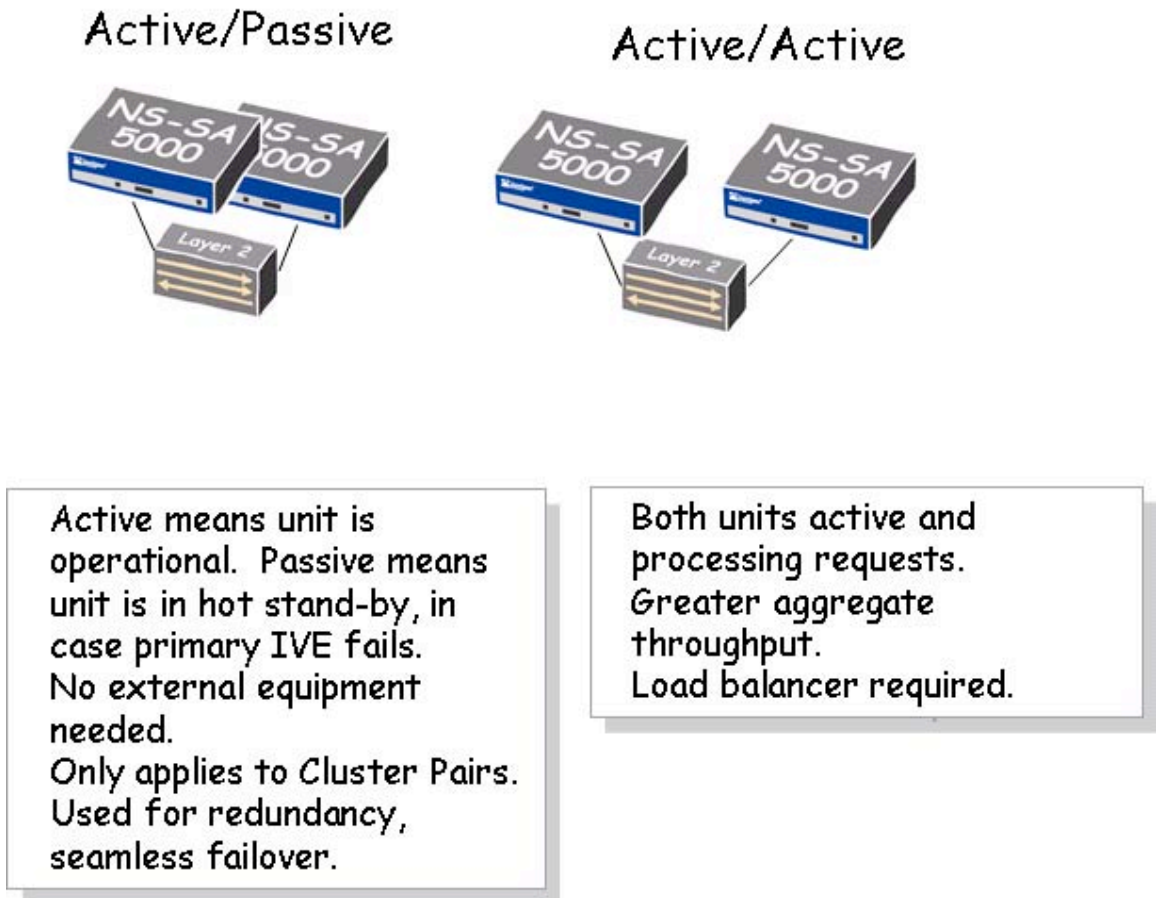
IVE platforms are designed to provide various stateful clustering options, offering high availability across the LAN and the WAN. The IVE can be deployed in clusters of two units or more to provide continued access in the event of a system failure.

In the event of system failure, the user's session state is maintained, even if the physical unit that failed is the one they used to begin their session.

The HA options for IVE are shown below.

¹ For a detailed discussion on high availability options for routers and firewalls, see *High Availability at the Central Site Edge* at www.juniper.net.

Figure 9: HA Options for IVE



With Active/Passive high availability, Active means the unit is operational. Passive means the unit is in hot stand-by, in case the primary IVE fails. No external equipment is needed for this configuration, which only applies to cluster pairs. This provides a seamless failover.

With the Active/Active option, all the units are active and processing requests. This provides greater aggregate throughput. A Layer 4 switch (or optionally a Juniper Networks DX application accelerator configured as a load balancer) is required for load balancing and failover.

HA for IDP

You can place IDP appliances in a HA cluster anywhere on the network. The first step in setting up the IDP system on your network is to determine where you want to install the IDP appliance and which high availability deployment mode you want to use for failure protection or load balancing.

You can deploy IDP appliances in bridge, router, transparent, or proxy-ARP mode to enable a high availability solution. In the network described in this application note we are using transparent mode.

For more information on the deployment and high availability options for IDP appliances, see the *Intrusion Detection and Prevention Concepts and Examples Guide* and the *IDP High*

Availability Quickstart Guide at www.juniper.net.

HA for DX

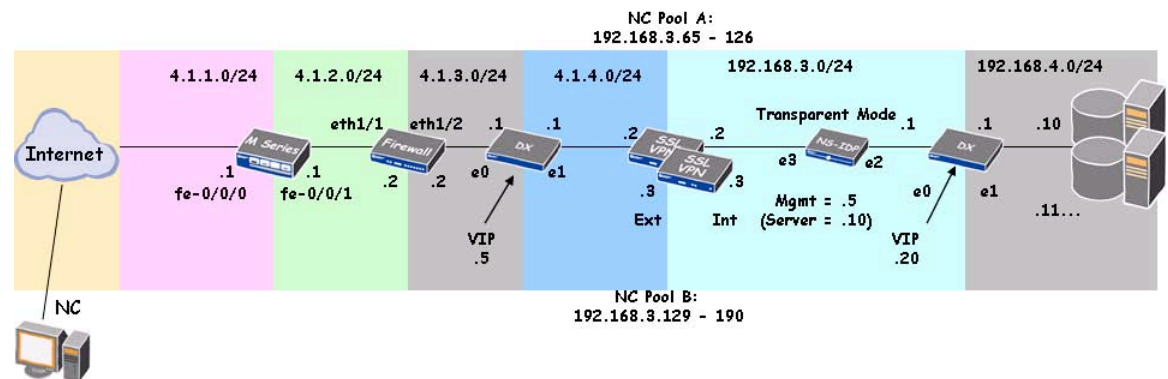
The DX application acceleration device can be deployed in three different topologies to increase system availability: Active/Standby, Active/Active, or ActiveN. Appliances arranged in an ActiveN (cluster) topology not only perform Server Load Balancing, they also perform health checking and automatic failover when an unavailable appliance is detected.

The *Configuring for High Availability* chapter of the *DX Installation and Administration Guide* provides an overview of the three different topologies used to increase system availability.

Network Diagram

A diagram for this test is shown below.

Figure 10: Network Diagram



This solution shows a complete extended enterprise at the central site perimeter, including router, firewall, application load balancer, secure access, IDP and application accelerator. The configuration of this solution is discussed in the following sections.

Configuration of the Solution

Configuration of this solution follows.

Router and Firewall

In this test, the router and firewall are configured with rudimentary settings just to show a complete solution. In the case of the router, we are just implementing a static route to the firewall, and the firewall simply sets static routes to DX and a default gateway to the router.

Naturally, in a production setting, a dynamic routing protocol such as OSPF would probably be used on the router and the firewalls would be set up with multiple zones and policies to define traffic rules between these zones. For more information, see the *Central Site Edge*

Solution Brief and High Availability at the Central Site Edge at www.juniper.net.

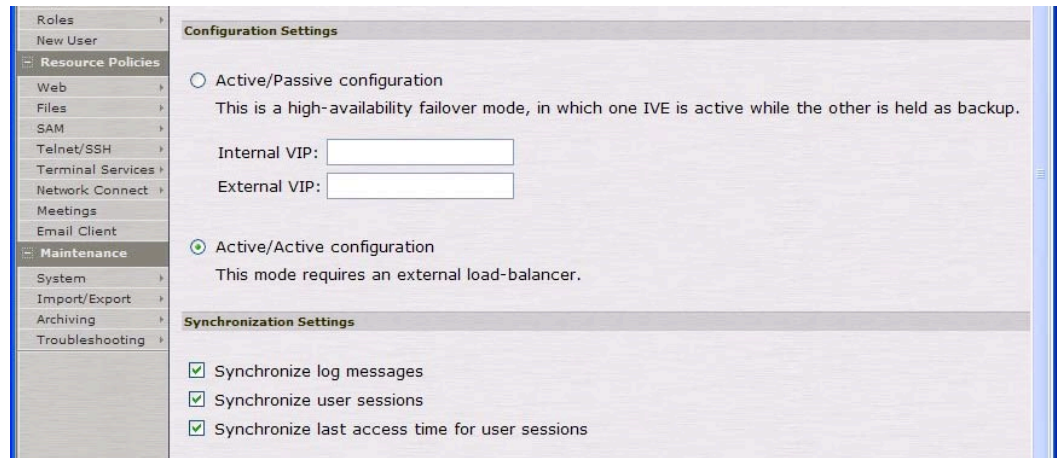
Router and Firewall Configurations can be found in Appendix B.

IVE

The cluster properties for the IVE follow. Note that the IVE is in an Active/Active cluster configuration. It is being load balanced by DX-A.

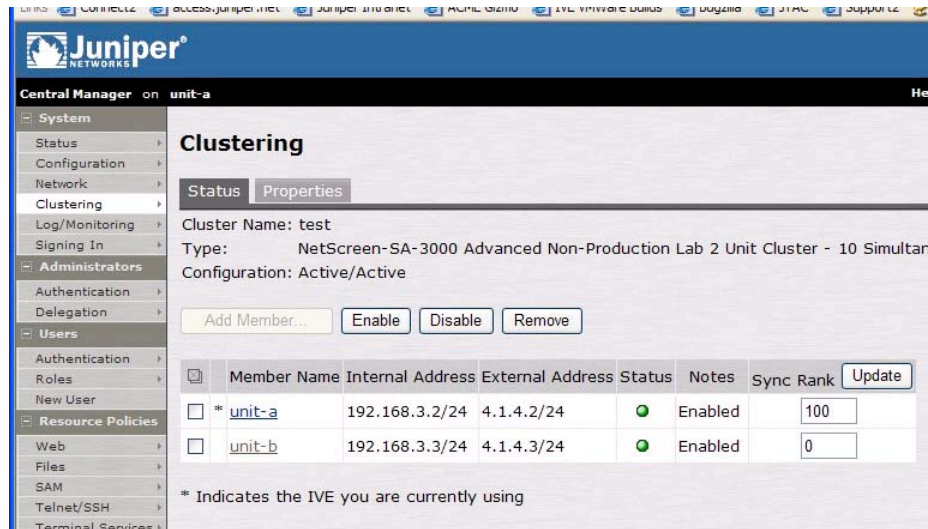
Note: Since we are configuring the DX for Half-NAT operation, the External Default Gateway for each unit must point to the external DX-A SLB.

Figure 11: Cluster Configuration for IVE (Active/Active)



The following screen shows the clustering for the SA cluster. It demonstrates the IP addressing and the Sync Ranking, which specifies the synchronization order for nodes when joining a cluster. The highest rank (in this case, 100) takes precedence.

Figure 12: Clustering



Central Manager on unit-a

Clustering

Status Properties

Cluster Name: test
 Type: NetScreen-SA-3000 Advanced Non-Production Lab 2 Unit Cluster - 10 Simultar
 Configuration: Active/Active

Add Member... Enable Disable Remove

	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
<input type="checkbox"/>	* unit-a	192.168.3.2/24	4.1.4.2/24	● Enabled		100	
<input type="checkbox"/>	unit-b	192.168.3.3/24	4.1.4.3/24	● Enabled		0	

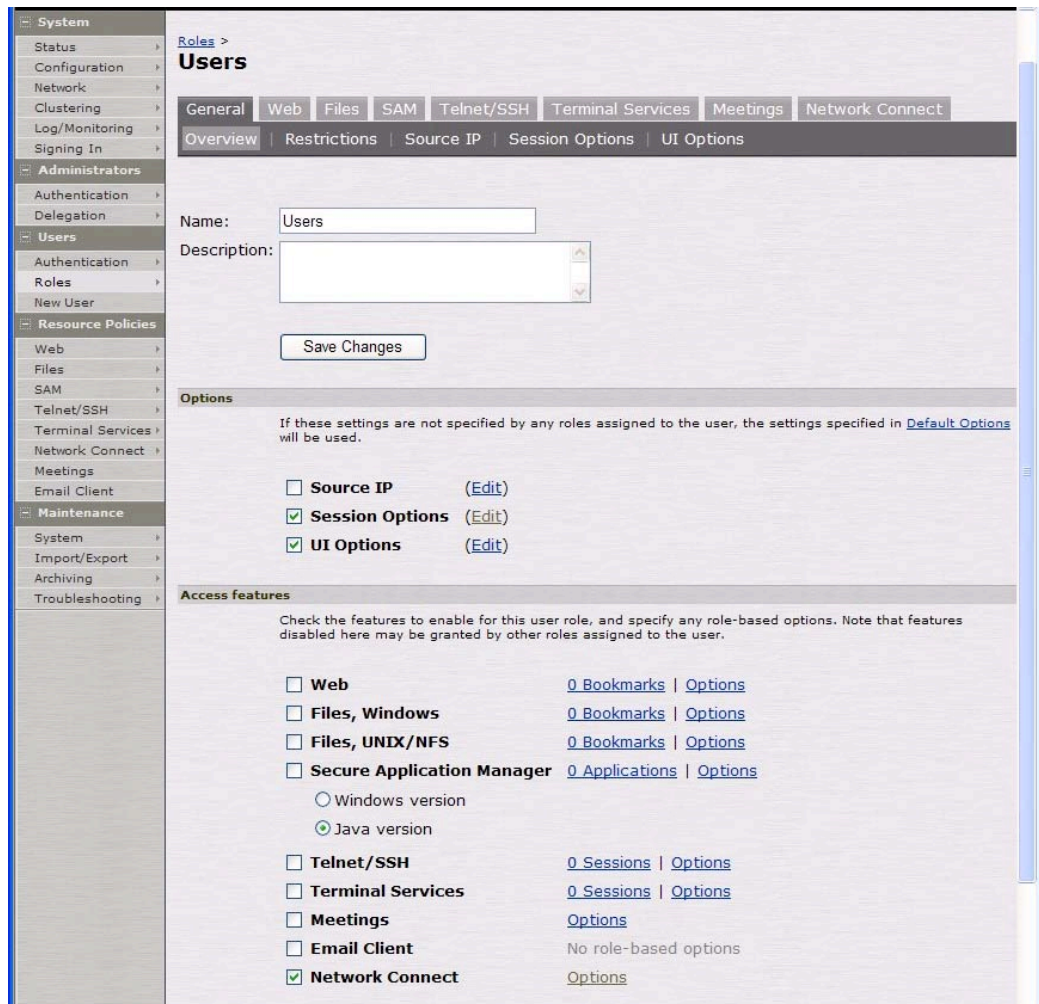
* Indicates the IVE you are currently using

The following screen shot shows the NC Connection Profiles. This creates an NC resource profile. When an IVE receives a client request to start an NC session, the IVE assigns an IP address to the client-side NC agent. This address is based on the IP address pool policies that apply to a user's role. You also specify the transport protocol here, as well as encryption method, and whether or not to employ data compression for the NC session. In this case, we specify the address pool for each SA-3000, and indicate that the default transport will be IPsec (ESP).

NC IP Pools can be assigned from the same subnet as the internal interface, in which case the IVE will respond to ARP requests on behalf of those IP addresses, and no additional configuration is required. Alternatively, NC IP Pools can be assigned arbitrary subnet ranges as long as the next hop router has a static route installed for those subnets with a next hop pointing back to the IVE. These static routes should be redistributed into the rest of the corporate network for full connectivity.

The following figure shows the general Roles, indicating that users will be connecting via NC.

Figure 13: General IVE Roles



Next you configure the NC page. You use the NC tab to specify split-tunneling, auto-launch, auto-uninstall, and Graphical Identification and Authentication (GINA) options for a role. The following screenshot shows the roles for NC users in this network.

Figure 14: NC Roles

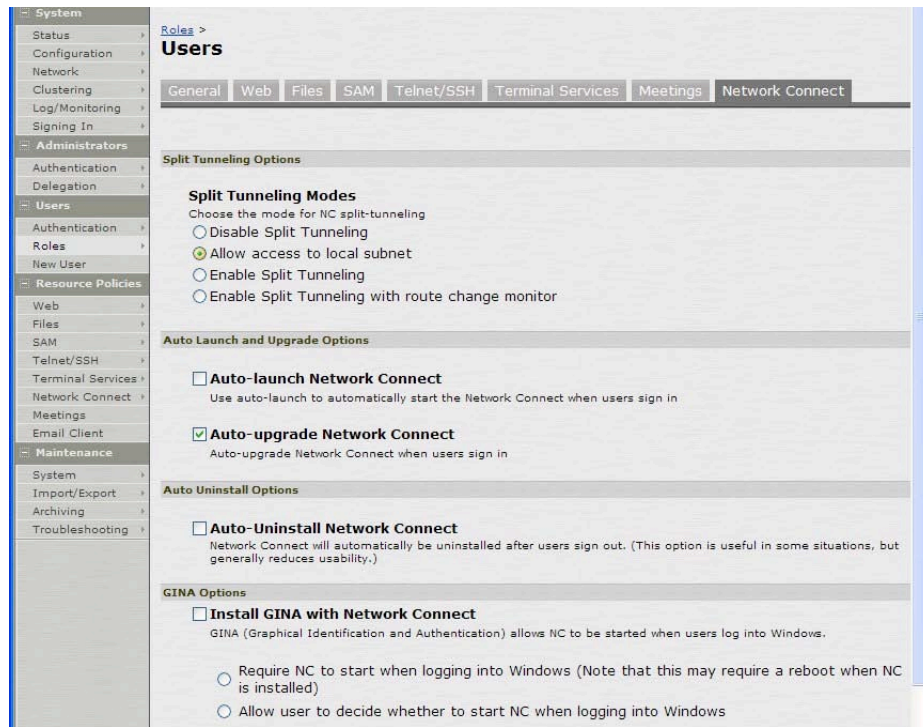
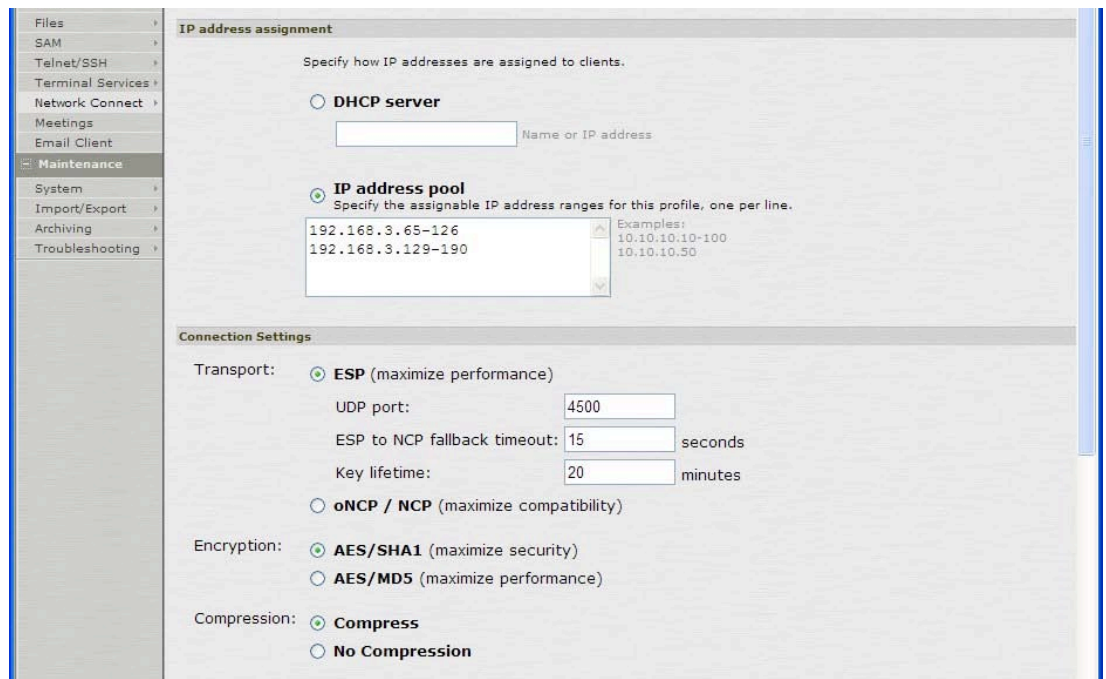
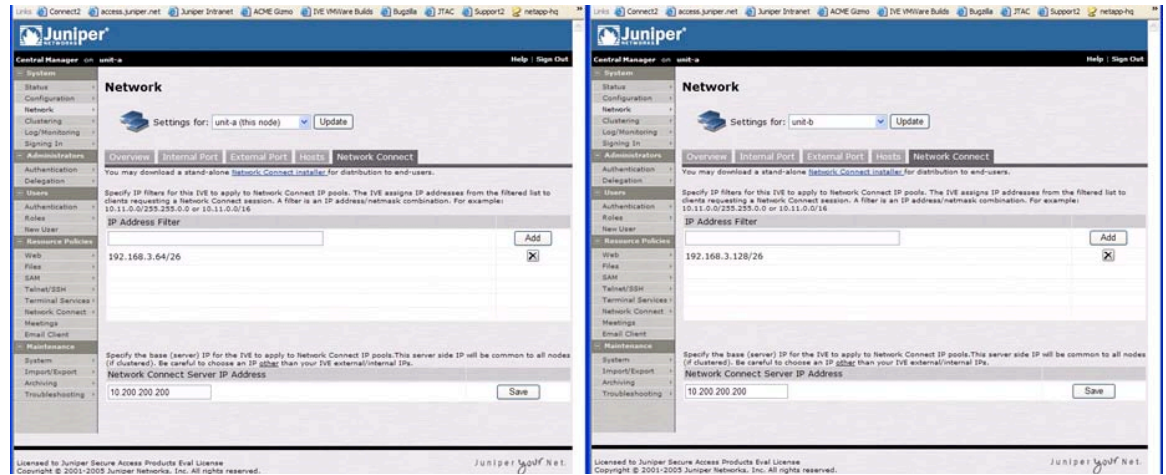


Figure 15: NC Profile



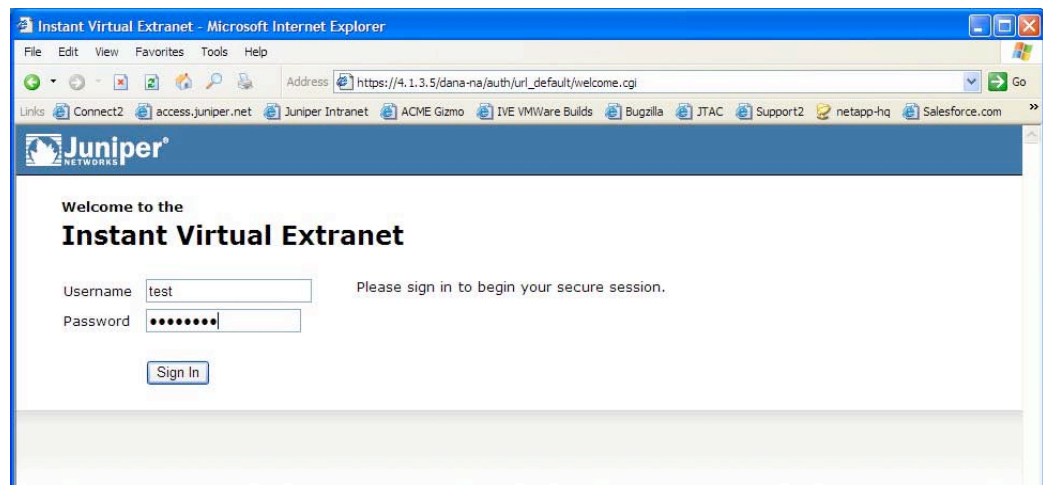
The following figure shows the NC IP Pool filters for NC-A and NC-B (the two SA-3000 units). NC filters are required for Active/Active cluster configurations so each unit will assign the appropriate IP addresses to NC clients when they connect. This keeps NC client IP addresses from conflicting within the cluster and allows the next hop router to forward packets to the correct unit in the cluster.

Figure 16: Addressing for NC-A and NC-B



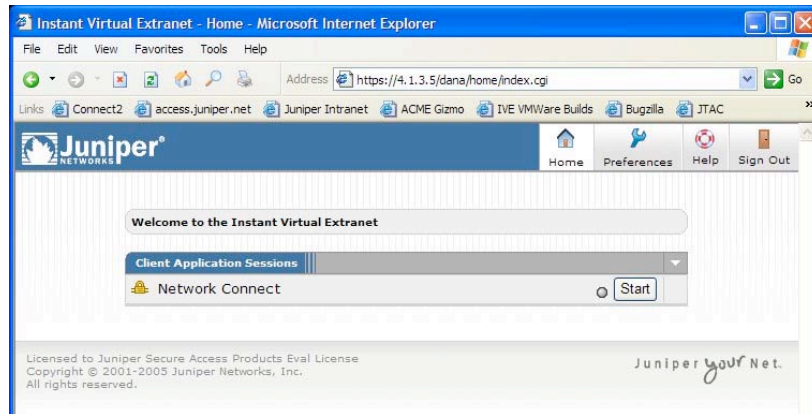
The user login for the IVE follows.

Figure 17: User Login



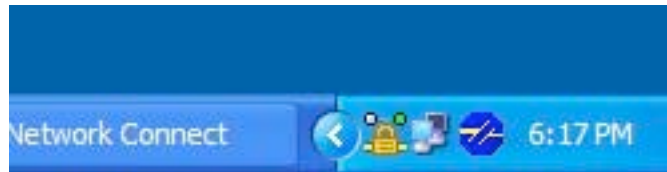
When your login is successful you see the following banner.

Figure 18: IVE Banner



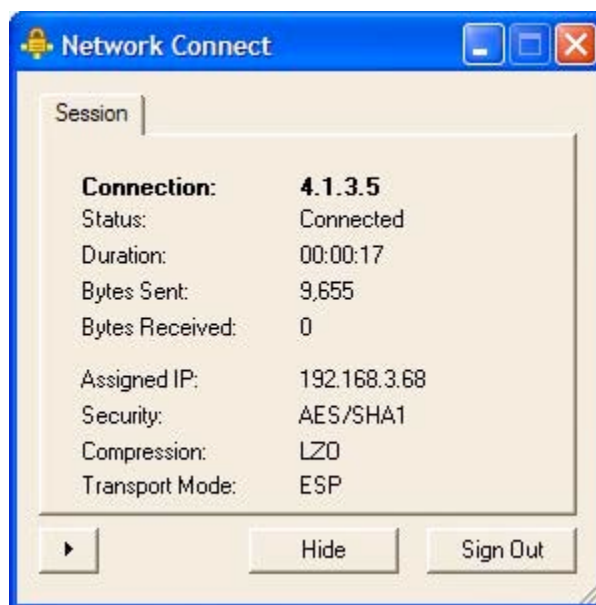
When NC is connected you see the following on your task tray.

Figure 19: NC Task Tray



Click on the NC icon and you see the following connection information.

Figure 20: NC Connection Status

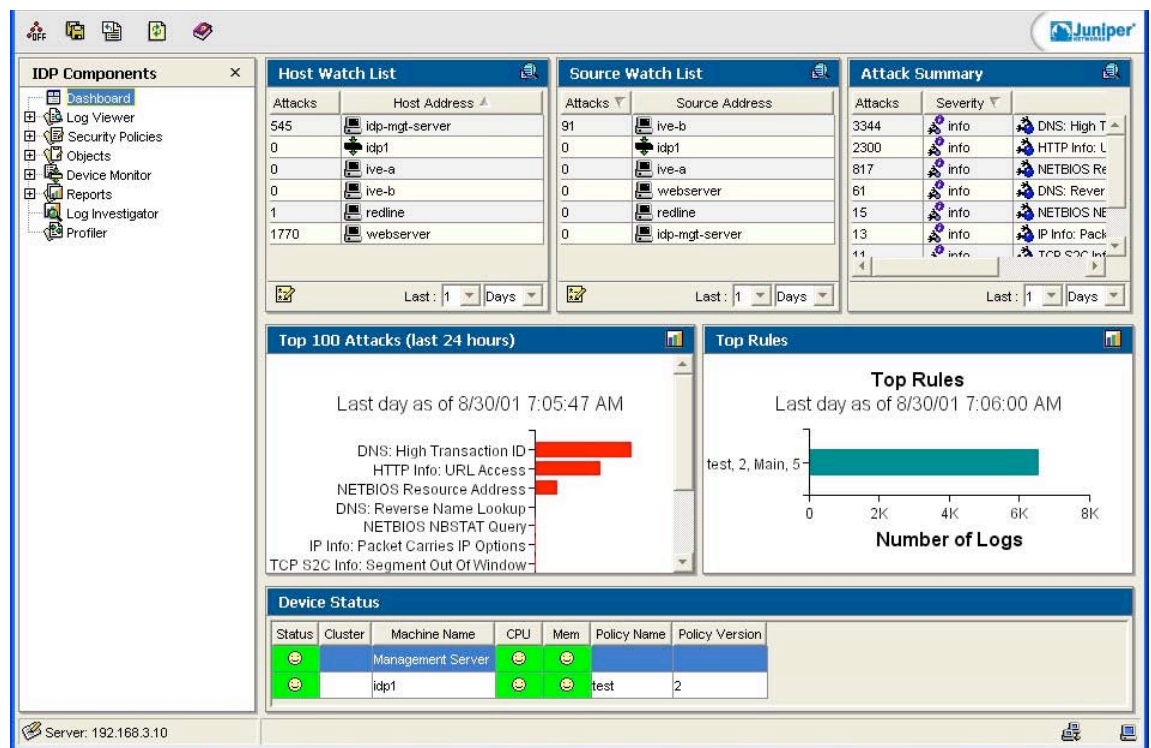


IDP in Transparent Mode

The IDP is set up in transparent mode rather than routed mode. In this mode, both forwarding interfaces for each IDP appliance are stealth interfaces, indicating that they do not have an assigned IP address. This configuration reliably responds to and prevents attacks, and is a simple transparent deployment. There are no changes needed to routing tables or to network equipment. However, there is a limitation in that high availability is available only in a “hot standby” mode.

A typical IDP configuration includes a management server, the IDP sensor, and the user interface. The user interface includes the IDP dashboard, shown in the following figure.

Figure 21: IDP Dashboard

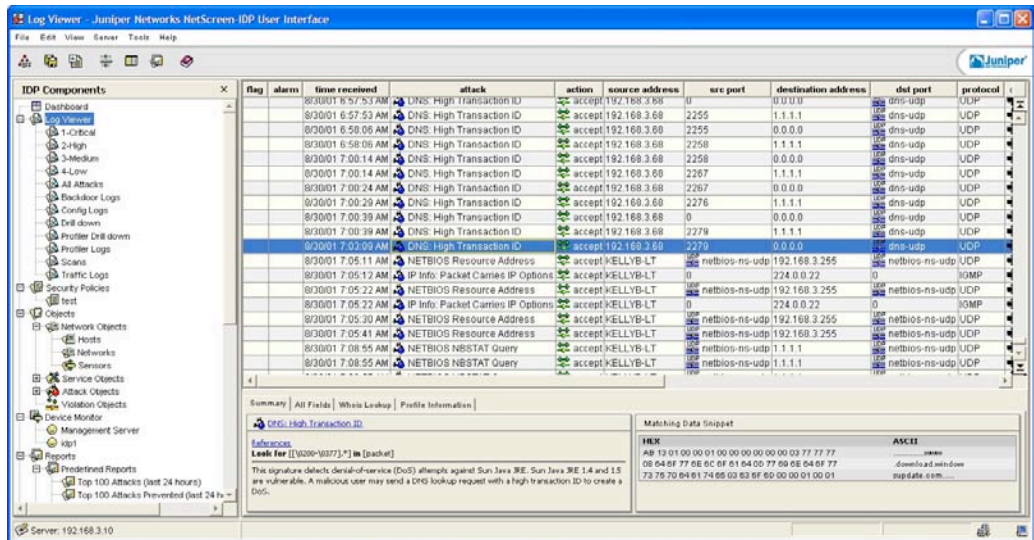


The Dashboard displays the vital statistics of your network and the IDP system. It is the default component shown in the main display area when you first log in. You use the data provided in the Dashboard to make quick, at-a glance decisions about how to employ IDP.

The data that appears in the Dashboard is real time and refreshes periodically from the IDP Management Server. You can customize the Dashboard to display only the information that is most important to you and your network.

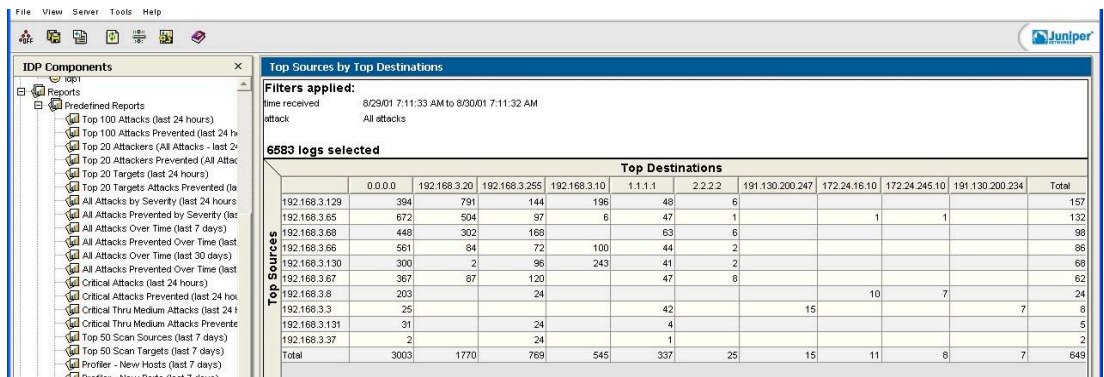
Another part of the user interface is a Log Viewer, which you can use to view log records that IDP Sensors generate based on criteria defined in the Security Policies. The Log Viewer displays log records in table format and can be modified using filters or column settings. The Log Viewer is shown in the following figure.

Figure 22: Log Viewer



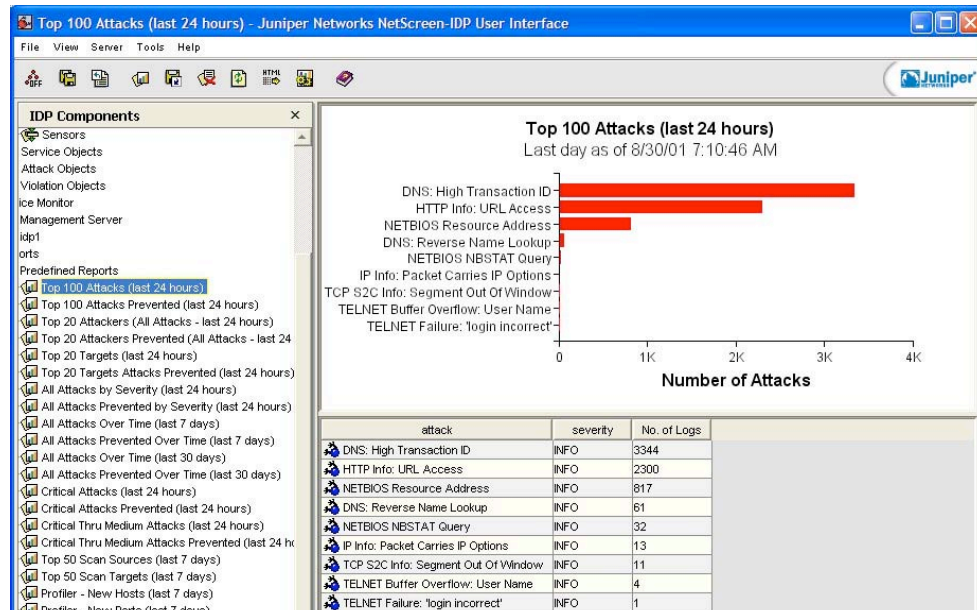
The IDP UI also includes a Log Investigator, which provides a method of drilling down into filtered log record data by correlating log record information with particular criteria. The following screen shot shows top source and destination IP addresses.

Figure 23: IDP Log Investigator



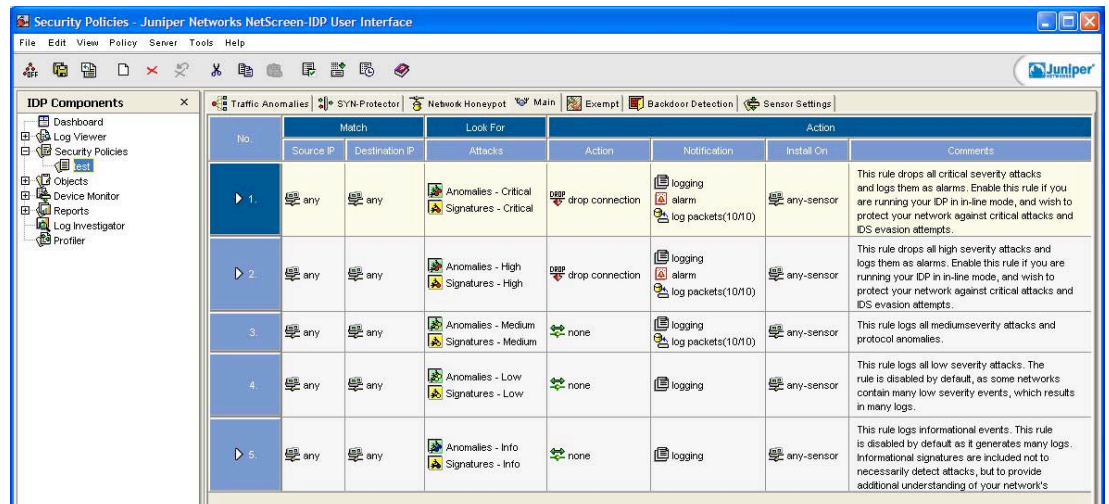
The IDP user interface includes a Reports feature (following figure), which provides a high-level overview and summaries of the log record data generated by the Sensors deployed in your network. You can use reports to view log data in tabular or graphical form.

Figure 24: IDP Reports



Security Policies, rule bases, and rules are the core of the IDP system. Rules are basic instructions that direct the behavior of the IDP Sensor. You can have multiple rules; rules are organized into rule bases. The rule set used for this network follows.

Figure 25: Rule Base



DX Load Balancing (DX-A)

Interesting aspects of the DX configuration follow.

Use of Half-NAT

Traffic flows for load balancing may undergo either Full or Half-NAT translation. With Half-NAT, only the destination IP address is changed; with Full-NAT, both the source and destination IP addresses are rewritten.

The use of Half-NAT allows the DX to preserve source addressing. This is more flexible approach and simpler to troubleshoot. This allows the remote users' source IP addresses to be visible to the IVE, which allows the Administrator to see meaningful log entries and do source-based filtering if desired. Most users will probably want to set it up this way.

Note that a Half-NAT configuration on the DX requires each unit in the IVE cluster to be configured to use the DX as the default gateway for the External interface.

Connectivity to the VIP

High Availability mode for the DX is achieved through the use of a Virtual IP address (VIP).

Note: You must use E0 as the external interface on the DX; otherwise, the VIP will not respond to ARP requests.

SLB Groups

Round robin load balancing was used in this test. The DX also supports least connection and weighted round robin load balancing.

Note: You need to set the Redline SLB Active Session timeout above the default of 100 seconds (120 is fine). For example, you can enter **set slb session timeout active 120**. This will ensure proper operation of NC.

When setting up SLB groups for NC in IVE 5.0, you need to set up three groups: one each for IPSec, SSL, and HTTP.

```

=====
group ssl
vip: 4.1.3.5
port: 443
policy: roundrobin
protocol: tcp
nat: half
sticky: enabled
smtp healthcheck: disabled

Targethosts:
Ip:Port          Weight  Maxconn  Status
-----
4.1.4.2:443      1       200      Up
4.1.4.3:443      1       200      Up
-----
=====
=====
group ipsec
vip: 4.1.3.5

```

```

port: 4500
policy: roundrobin
protocol: udp
nat: half
sticky: enabled
smtp healthcheck: disabled

Targethosts:
Ip:Port          Weight  Maxconn  Status
-----
4.1.4.2:4500     1       200      Up
4.1.4.3:4500     1       200      Up
-----
=====
group http
vip: 4.1.3.5
port: 80
policy: roundrobin
protocol: tcp
nat: half
sticky: enabled
smtp healthcheck: disabled

Targethosts:
Ip:Port          Weight  Maxconn  Status
-----
4.1.4.2:80       1       200      Up
4.1.4.3:80       1       200      Up
-----

```

Note: Layer 7 health-checking on the DX is limited to SMTP in SLB mode. There is a scripting mechanism to selecting perform health checking for other protocols. Full Layer 3 and Layer 4 health checking is available.

DX Application Acceleration (DX-B)

The application acceleration in this lab is very simple. It consists of a very basic cluster configuration on DX-B to accelerate back end web servers.

A portion of the cluster configuration follows.

```

----- Clusters -----
Cluster [1]
Description:
# Internal VIP for Back-end Apps
Listen Address: 192.168.3.20
Listen Netmask: 255.255.255.255
<snip>
# Client IP will stay with the same server
Sticky Method: clientip
<snip>
# Server Host Addresses Follow
TargetHosts:

```

```
192.168.4.10:80 (enabled)
192.168.4.11:80 (enabled)
Cache: None.
```

The entire cluster configuration is available in *Appendix B* under DX-B.

Note: The IDP should be placed in front of the Application Acceleration device. This way the DX is only processing valid traffic.

For more information on application acceleration, see the DX Installation and Administration Guide at www.juniper.net.

Conclusion

This extended enterprise solution includes the IVE 5.0 Secure Access architecture, configured in high availability mode and load balanced by the DX application accelerator. It also includes the Juniper Networks Intrusion Detection and Prevention (IDP) platform, and a second DX to optimize user sessions and accelerate applications.

Appendix A: Sizing a Deployment

The science of sizing an Instant Virtual Extranet deployment with Secure Access is more of an “art” and less of a science. Some rules of thumb follow.

For employee remote access only, 10:1 or 6:1 ratios are most commonly used (meaning you should assume this ratio of total users will need to be connected via IVE). However, very few deployments of Secure Access are for pure employee remote access, meaning the Extranet is equally important and the named users can grow much larger. Thus, if you add all of the customers, business partners, contractors, and employees via Secure Access, the ratio could vary significantly.

As a rule, Juniper usually uses 10 to 1 for named users to concurrent users as an estimation tool.

Then there is the question of bandwidth allocation. This is generally less of an issue because many users are coming in over DSL, cable modem, or a fractional leased line. Further, the uplink speeds on those remote users are generally much less than a full T1/DS-1; beyond that, the application bandwidth requirements (email, Intranet, file sharing, etc.) are generally less than 160 kbps (20KB/s).

Thus, guidelines indicate it is safe to assume ~20kbps for average and ~160kbps for peak bandwidth consumption. For example, when using SA-5000 with 2500 concurrent users:

- 2500 users (peak) * 160kbps (peak) = ~400Mbps
- 2500 users (peak) * 20kbps (average) = ~50Mbps
- 1200 users (50% peak) * 160kbps (peak) = ~192Mbps
- 1200 users (50% peak) * 20kbps (average) = ~24Mbps [typical peak load]
- 250 users (25% peak) * 20kbps (average) = ~5Mbps [typical average load]

Appendix B: Configurations

Configurations follow.

Edge Router

```
version 7.2R1.7;
system {
  services {
    web-management {
      http;
    }
  }
  syslog {
    user * {
      any emergency;
    }
    file messages {
      any any;
      authorization info;
    }
    file interactive-commands {
      interactive-commands any;
    }
  }
}
interfaces {
  fe-0/0/0 {
    unit 0 {
      family inet {
        address 4.1.1.1/24;
      }
    }
  }
  fe-0/0/1 {
    unit 0 {
      family inet {
        address 4.1.2.1/24;
      }
    }
  }
}
/* Static route to firewall */
routing-options {
  static {
    route 4.1.3.0/24 next-hop 4.1.2.2;
    route 4.1.4.0/24 next-hop 4.1.2.2;
  }
}
```

Firewall

```
# Begin ScreenOS Configuration

# Define Virtual Routers
```

```
set vrouter trust-vr sharable

#Establish Network Connect Service
set service "nc" protocol udp src-port 1-65535 dst-port 4500-4500

#Establish Trust and Untrust Zones
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block

#Establish Attack Screenings for Untrust Zones
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land

#Set zone, IP and NAT for Trust and Untrust
set interface "ethernet1/1" zone "Untrust"
set interface "ethernet1/2" zone "Trust"
set interface ethernet1/1 ip 4.1.2.2/24
set interface ethernet1/1 route
set interface ethernet1/2 ip 4.1.3.2/24
set interface ethernet1/2 nat

#Set management settings
set interface mgt ip 192.168.1.1/24
set interface ethernet1/1 ip manageable
set interface ethernet1/2 ip manageable
set interface ethernet1/1 manage ping
set interface ethernet1/1 manage ssh
set interface ethernet1/1 manage telnet
set interface ethernet1/1 manage snmp
set interface ethernet1/1 manage ssl
set interface ethernet1/1 manage web

#Establish route to DX
set address "Trust" "dx" 4.1.3.5 255.255.255.255

#Set policies for Untrust to Trust for SSL, HTTP and NC
set policy id 1 from "Untrust" to "Trust" "Any" "dx" "HTTP" permit
set policy id 2 from "Untrust" to "Trust" "Any" "dx" "HTTPS" permit
set policy id 3 from "Untrust" to "Trust" "Any" "dx" "nc" permit

#Set virtual routers
set vrouter "untrust-vr"
set vrouter "trust-vr"

#Set static route to DX and default gateway to Router
set route 4.1.4.0/24 interface ethernet1/2 gateway 4.1.3.1
set route 0.0.0.0/0 interface ethernet1/1 gateway 4.1.2.1

#End ScreenOS Configuration
```

DX – A (Load Balancing)

```
----- Version -----
E|X Version: 4.1.25    Build ID: 0

----- Hostname, Date, & Time -----
Timezone: America/Los_Angeles
NTP server1: 192.168.0.2
NTP: down

----- Network -----
Domain: xxxxxxxxxxxxxxxx.com
Nameserver1: 192.168.0.2
ether0: IP address = 4.1.3.1 netmask = 255.255.255.0
ether0: Broadcast = 4.1.3.255
ether0: MAC = 00:e0:81:23:1e:66 VMAC = (unconfigured) MTU = 1500
ether0 media: 100baseTX full-duplex (100baseTX full-duplex) Status: active
ether0 supported media options:
  [1] 10baseT/UTP
  [2] 10baseT/UTP full-duplex
  [3] 100baseTX
  [4] 100baseTX full-duplex
  [5] autoselect
ether1: IP address = 4.1.4.1 netmask = 255.255.255.0
ether1: Broadcast = 4.1.4.255
ether1: MAC = 00:e0:81:23:1e:67 VMAC = (unconfigured) MTU = 1500
ether1 media: 100baseTX full-duplex (100baseTX full-duplex) Status: active
ether1 supported media options:
  [1] 10baseT/UTP
  [2] 10baseT/UTP full-duplex
  [3] 100baseTX
  [4] 100baseTX full-duplex
  [5] autoselect
Default route: 4.1.3.2

----- Clusters -----

----- Forwarders -----

----- Redirectors -----

----- Server -----
CustomIPLogHeader:
Custom Client Certificate Header: CLIENT_CERT
Failover Status: disabled
Failover Link Fail Poll Interval: 500
Failover Link Fail Count: 4
Failover Virtual MAC Status: disabled
Failover Virtual MAC Id: 0
Max Conns: 50000
Reverse path route: disabled
Reverse path route maximum routes: 20
Reverse path route timeout: 45
Server: up

----- Admin Interface -----
Admin Interface:
VIP Address:
VIP Netmask: 255.255.255.255
```

```
----- Web UI -----  
Port: 8090  
SSL Status: disabled  
SSL Keyfile:  
SSL Keypass: none  
SSL Certfile:  
Session Expire Time: 900  
Web UI: up
```

```
----- SOAP -----  
Port: 8070  
SSL Certfile: democert  
SSL Keyfile: demokey  
SSL Keypass: none  
SOAP server: up
```

```
----- CLI -----  
Cli Session Expire Time: 600
```

```
----- SNMP -----  
System Contact: Unknown  
System Location: Unknown  
Community Name: public  
Community IP: 192.168.0.0  
Community Netmask: 255.255.0.0  
Trap Host 1 IP:  
Trap Host 1 Community:  
Trap Host 1 Version:  
Trap Host 2 IP:  
Trap Host 2 Community:  
Trap Host 2 Version:  
Generic Traps: disabled  
Enterprise Traps: disabled  
Authentication Failure Trap: disabled  
Trap Connection Threshold: 100  
SNMP: down
```

```
----- Terminal Services -----  
SSH: up  
Telnet: up
```

```
----- Email -----  
SMTP server:  
Email address:  
  From address:  
  Default 'to' address:
```

```
----- Audit Log -----  
Show cmds admin logging: disabled
```

```
----- System Log -----  
Logging: enabled  
Logging to:  
  email: (none)  
  memory: ALERT
```

```
syslog: (none)
console: (none)
Email 'mailto' addresses:
  mailto1:
  mailto2:
Logging Facility: LOG_USER
SyslogHost1:
SyslogHost2:
SyslogPort: 514

----- Upgrade/Install -----
Upgrade Filename:
Upgrade Transport: tftp

----- TCPDump -----
transport: tftp
filename:
mailto1:
mailto2:

----- TSDump -----
transport: tftp
filename:
mailto1:
mailto2:

----- File Transfer -----
SCP Server:
SCP UserName:
TFTP Server:

----- ActiveN -----
ActiveN basic Configuration
=====
Reap Timeouts(in Secs):
Active: 100
Close: 25
Ack Wait(syn flood): 10

Cleaning Interval: 13 secs
Blade Max: 16
Sticky timeout: 120 (minutes)

HealthCheck Params
Timeouts(In secs):
Up: 45
Down: 20
Syn wait: 10
Max tries(before fail): 3
SourceIP for local HC:
Switch Status: disabled

Active N advanced Configuration
=====
Switching policy: Round Robin
SynFlood Protect: no
```

```
Burst Max: 7000
Reset to server on purge: yes
Reset to client on purge: yes

Failover: disabled
Mcast addr: 239.0.0.1
Bind addr: not configured
Node Id: auto
Peer Port: 9200
Force master: disabled
Vmac: disabled
My node: -1
Failover state: activeN disabled

----- SLB -----
Server Load balancer basic Configuration
=====
Reap Timeouts(in Secs):
# Set Active to 120 to ensure correct NC operation
Active: 120
Close: 12
Ack Wait(syn flood): 6

Reset to client: enabled
Reset to server: enabled

Sticky idle timeout: 120

HealthCheck Params
Timeouts(In secs):
Up: 1
Down: 1
Syn wait: 1
Max tries(before fail): 1
Switch Status: enabled (stand-alone)

=====
group ssl
vip: 4.1.3.5
port: 443
policy: roundrobin
protocol: tcp
nat: half
sticky: enabled
smtp healthcheck: disabled

Targethosts:
Ip:Port          Weight  Maxconn  Status
-----
4.1.4.2:443      1       200      Up
4.1.4.3:443      1       200      Up
-----
=====
group ipsec
vip: 4.1.3.5
port: 4500
```

```
policy: roundrobin
protocol: udp
nat: half
sticky: enabled
smtp healthcheck: disabled

Targethosts:
Ip:Port          Weight  Maxconn  Status
-----
4.1.4.2:4500     1       200      Up
4.1.4.3:4500     1       200      Up
-----
=====
group http
vip: 4.1.3.5
port: 80
policy: roundrobin
protocol: tcp
nat: half
sticky: enabled
smtp healthcheck: disabled

Targethosts:
Ip:Port          Weight  Maxconn  Status
-----
4.1.4.2:80       1       200      Up
4.1.4.3:80       1       200      Up
-----
=====
Failover: disabled
Mcast addr: 239.0.0.2
Bind addr: not configured
Node Id: auto
Peer Port: 9200
Force master: disabled
Vmac: disabled
My node: -1
Failover state: standalone
```

IVE (Secure Access 3000)

IVE configuration is discussed in the “Configuration of the Solution” section above.

IDP

IDP configuration is discussed in the “Configuration of the Solution” section above.

DX – B (Application Acceleration)

```
E|X Version: 4.1.25    Build ID: 0

----- Hostname, Date, & Time -----
Hostname: www.xxxxxxxxxxxxxxxxx.com
```

```
2005.06.30 09:51:20 PDT
Timezone: America/Los_Angeles
NTP server1: 192.168.0.2
NTP: down

----- Network -----
Domain: xxxxxxxxxx.com
Nameserver1: 1.1.1.1
ether0: IP address = 192.168.3.1 netmask = 255.255.255.0
ether0: Broadcast = 192.168.3.255
ether0: MAC = 00:e0:81:21:49:68 VMAC = (unconfigured) MTU = 1500
ether0 media: 100baseTX full-duplex (100baseTX full-duplex) Status: active
ether0 supported media options:
  [1] 10baseT/UTP
  [2] 10baseT/UTP full-duplex
  [3] 100baseTX
  [4] 100baseTX full-duplex
  [5] autoselect
ether1: IP address = 192.168.4.1 netmask = 255.255.255.0
ether1: Broadcast = 192.168.4.255
ether1: MAC = 00:e0:81:21:49:69 VMAC = (unconfigured) MTU = 1500
ether1 media: 100baseTX full-duplex (100baseTX full-duplex) Status: active
ether1 supported media options:
  [1] 10baseT/UTP
  [2] 10baseT/UTP full-duplex
  [3] 100baseTX
  [4] 100baseTX full-duplex
  [5] autoselect
Default route: 192.168.3.1

----- Clusters -----
Cluster [1]
Description:
# Internal VIP for Back-end Apps
Listen Address: 192.168.3.20
Listen Netmask: 255.255.255.255
Listen Port: 80
Listen SSL Status: disabled
Listen SSL Protocol: sslv23
Listen SSL Certfile:
Listen SSL Keyfile:
Listen SSL Keypass: none
Listen SSL Ephemeral Keyfile:
Listen SSL Ephemeral Keypass: none
Listen SSL Ciphersuite: all
Listen SSL Cipherfile:
Client Authentication: disabled
CA Certfile:
CA CRL File:
CA Trust File:
Client Certificate Authentication Type: local
Client Certificate Forwarding: disabled
Client Certificate Forwarding Format: DERBase64
Listen TargetsDown Mode: blackhole
DSR Status: disabled
Health Check Status: disabled
Health Check Interval: 150
```

```
Health Check Retry: 4
Health Check Resume: 1
Health Check Url Path:
Health Check Return Code: 200
Health Check Size: -1
Health Check String:
Health Check Timeout: 15
Health Check User Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0;
T312461)
# Client IP will stick to the server
Sticky Method: clientip
Sticky Cookie Mask: ippport
Sticky Cookie Expire: 0
Sticky Client IP Distribution: internet
Sticky Client IP Timeout: 120
Convert 302 Protocol Status: disabled
Weblog Status: disabled
Weblog Destination: syslog
Weblog Format: common
Weblog Syslog Host:
Weblog Syslog Port: 514
Weblog Batch memory allocated for this cluster (in MB): 10
Total free memory available for all clusters: 50 MB
Weblog Batch Copy Time 1:
Weblog Batch Copy Time 2:
Weblog Batch Copy Time 3:
Weblog Batch Copy Interval: 0
Weblog Batch Retry Interval: 60
Weblog Batch Scp Directory:
Weblog Batch Scp Username:
Weblog Batch Scp Keyfile:
Weblog Batch Host:
Weblog Batch Compression: enabled
Weblog Delimiter: space
Connection Binding Status: disabled
Rule Set File:
AppRule Processing: disabled
AppRule Limit Retry Post: 32768
HTTP Authentication Status: disabled
HTTP Authentication Method: WWW
Authentication Realm:
Authentication Response Text:
HTTP Authentication Protocol: RADIUS
Authentication Redirect Status: disabled
Authentication Redirect Page URL: /auth.shtml
Authentication Redirect Host:
Authentication Redirect Protocol: http
Authentication Password MaxAge: 1
Authentication Password MaxLength: 8
HTTP Authentication Cache Status: enabled
Authentication Cache MaxAge: 60
RADIUS Server Key:
RADIUS Server Timeout: 10
RADIUS Server Retries: 3
RADIUS Server 1 IP:
RADIUS Server 1 Port: 1812
RADIUS Server 2 IP:
```

```
RADIUS Server 2 Port: 1812
HTTP Authentication Auditing: enabled
Audit Level: failures
OWA Status: disabled
Client IP Transparency: disabled
Targetname: www1.yourdomain.com
Target SSL Status: disabled
Target SSL Protocol: sslv23
Target SSL Certfile:
Target SSL Keyfile:
Target SSL Keypass: none
Target SSL Ciphersuite: common
Target SSL Cipherfile:
Target SSL Timeout: 1440
Target Local IP:
TargetHosts:
# Server Host Addresses Follow
 192.168.4.10:80 (enabled)
 192.168.4.11:80 (enabled)
Cache: None.

----- Forwarders -----

----- Redirectors -----

----- Server -----
CustomIPLogHeader:
Custom Client Certificate Header: CLIENT_CERT
Failover Status: disabled
Failover Link Fail Poll Interval: 500
Failover Link Fail Count: 4
Failover Virtual MAC Status: disabled
Failover Virtual MAC Id: 0
Max Conns: 50000
Reverse path route: disabled
Reverse path route maximum routes: 20
Reverse path route timeout: 45
Server: up

----- Admin Interface -----
Admin Interface:
VIP Address:
VIP Netmask: 255.255.255.255

----- Web UI -----
Port: 8090
SSL Status: disabled
SSL Keyfile:
SSL Keypass: none
SSL Certfile:
Session Expire Time: 900
Web UI: down

----- SOAP -----
Port: 8070
SSL Certfile: democert
```

```
SSL Keyfile: demokey
SSL Keypass: none
SOAP server: up

----- CLI -----
Cli Session Expire Time: 600

----- SNMP -----
System Contact: Unknown
System Location: Unknown
Community Name: public
Community IP: 192.168.0.0
Community Netmask: 255.255.0.0
Trap Host 1 IP:
Trap Host 1 Community:
Trap Host 1 Version:
Trap Host 2 IP:
Trap Host 2 Community:
Trap Host 2 Version:
Generic Traps: disabled
Enterprise Traps: disabled
Authentication Failure Trap: disabled
Trap Connection Threshold: 100
SNMP: down

----- Terminal Services -----
SSH: up
Telnet: up

----- Email -----
SMTP server:
Email address:
  From address:
  Default 'to' address:

----- Audit Log -----
Show cmds admin logging: disabled

----- System Log -----
Logging: enabled
Logging to:
  email: (none)
  memory: ALERT
  syslog: (none)
  console: (none)
Email 'mailto' addresses:
  mailto1:
  mailto2:
Logging Facility: LOG_USER
SyslogHost1:
SyslogHost2:
SyslogPort: 514

----- Upgrade/Install -----
Upgrade Filename:
Upgrade Transport: tftp
```

----- TCPDump -----

transport: tftp
filename:
mailto1:
mailto2:

----- TSDump -----

transport: tftp
filename:
mailto1:
mailto2:

----- File Transfer -----

SCP Server:
SCP UserName:
TFTP Server:

----- ActiveN -----

ActiveN basic Configuration
=====

Reap Timeouts(in Secs):
Active: 100
Close: 25
Ack Wait(syn flood): 10

Cleaning Interval: 13 secs
Blade Max: 16
Sticky timeout: 120 (minutes)

HealthCheck Params
Timeouts(In secs):
Up: 45
Down: 20
Syn wait: 10
Max tries(before fail): 3
SourceIP for local HC:
Switch Status: disabled

Active N advanced Configuration

=====

Switching policy: Round Robin
SynFlood Protect: no
Burst Max: 7000
Reset to server on purge: yes
Reset to client on purge: yes

Failover: disabled
Mcast addr: 239.0.0.1
Bind addr: not configured
Node Id: auto
Peer Port: 9200
Force master: disabled
Vmac: disabled

```
My node: -1
Failover state: activeN disabled

----- SLB -----
Server Load balancer basic Configuration
=====
Reap Timeouts(in Secs):
Active: 90
Close: 12
Ack Wait(syn flood): 6

Reset to client: enabled
Reset to server: enabled

Sticky idle timeout: 120

HealthCheck Params
Timeouts(In secs):
Up: 20
Down: 10
Syn wait: 5
Max tries(before fail): 3
Switch Status: disabled

Failover: disabled
Mcast addr: 239.0.0.2
Bind addr: not configured
Node Id: auto
Peer Port: 9200
Force master: disabled
Vmac: disabled
My node: -1
Failover state: SLB disabled
```

Copyright © 2005, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.