Deployment Guide for Microsoft Exchange 2010

Securing and Accelerating Microsoft Exchange with Palo Alto Networks Next-Generation Firewall and Citrix NetScaler Joint Solution
# Table of Contents

1. Overview .......................................................................................................................... 3
   1.1 Best-in-Class Solution for Microsoft Exchange 2010 ......................................................... 3

2. Requirements ...................................................................................................................... 4

3. Microsoft Exchange Server Network Topology ................................................................. 4
   3.1 Environment diagram ...................................................................................................... 4
   3.2 IP allocations ................................................................................................................ 5

4. Microsoft Exchange Installation and Configurations ......................................................... 5
   4.1 NetScaler Configuration ................................................................................................. 6
   4.2 Step-by-Step Installation .............................................................................................. 7

5. Deployment Instructions .................................................................................................... 8
   5.1.1 Add NSIP, Subnet Mask, and Default Gateway on NetScaler: ........................................ 8
   5.1.2 NetScaler Configuration by Using the Configuration Utility ........................................... 8
   5.1.3 Setup Wizard ............................................................................................................ 9
   5.2 NetScaler License installation ....................................................................................... 11
   5.3 NetScaler Basic Feature Setting ................................................................................... 12
     5.3.1 Systems Settings .................................................................................................. 12
     5.3.2 Basic Features ...................................................................................................... 12
   5.4 NetScaler AppExpert Outlook Web Access Template Install ........................................ 13
   5.5 NetScaler SSL Security Certificate installation (Self-Signed Certificate example) ............... 17
     5.5.1 Root-CA Certificate ............................................................................................. 17
     5.5.2 Server Certificate ............................................................................................... 21
   5.6 Creating virtual servers (VIP) ..................................................................................... 25
     5.6.1 HTTP VIP ........................................................................................................... 25
     5.6.2 HTTPS VIP .......................................................................................................... 27
   5.7 Creating a Service Group ............................................................................................... 30
   5.8 IMAP4 installation ........................................................................................................ 33
   5.9 POP3 installation .......................................................................................................... 36
   5.10 SMTP installation ....................................................................................................... 40
   5.11 Outlook Anywhere, ActiveSync confirmation ............................................................ 42

6. Services Verifications ......................................................................................................... 42
   6.1 Network IPs and Virtual IPs ....................................................................................... 42
   6.2 SSL Offload – Servers, Service Groups ......................................................................... 43
   6.3 Load Balancing – Servers, Service Group ..................................................................... 46
   6.4 Content Switching ........................................................................................................ 49

7. Monitoring – NetScaler Dashboard .................................................................................... 50
   7.1 By Service Groups ....................................................................................................... 50
   7.2 Per Server .................................................................................................................... 53

8. Palo Alto Networks Next-Generation Firewall Deployment ............................................. 56
   8.1 Data Center Segmentation ......................................................................................... 56
   8.2 Security Policy ............................................................................................................ 57
   8.3 User Identification ...................................................................................................... 63
   8.4 Threat Protection ....................................................................................................... 63

9. References ......................................................................................................................... 66
1. Overview

Business productivity hinges on providing users of IT resources secure access to the right applications and the right content – on demand. Enterprise IT strategies are rapidly evolving to support a world in which any user can safely access any application or data, using any device, from any location.

One of the biggest impediments in achieving this degree of flexibility is the enterprise network. Legacy networks were built to provide highly reliable connectivity between users, hosts, and networks, but with no awareness or context of application-layer traffic. This inherently limits the ability of the network to deliver to users the secure and transparent access to apps, data and virtual desktops they need to be productive, and to protect the organization from attack. What is required is a new approach – a next-generation cloud network that safely enables applications with the best-in-class performance and availability.

Palo Alto Networks and Citrix have come together to deliver best-in-class functionality upon which enterprises can build next-generation cloud networks. In addition to sharing a common vision of which networks must evolve, each company is delivering best-in-class solutions that already meet these requirements.

1.1 Best-in-Class Solution for Microsoft Exchange 2010

Citrix® NetScaler® and Palo Alto Networks take a best-in-class approach to optimizing and securing applications. This approach ensures the best total cost of ownership (TCO), security, availability, and performance for enterprise applications. The combined solution is a comprehensive network system that takes the best of high-speed load balancing, content switching, state-of-the-art application acceleration, layer 4-7 traffic management, data compression, dynamic content caching, SSL acceleration, network optimization, deep packet inspection, and next-generation network security to provide a robust, tightly integrated solution. Deployed in front of application servers, the NetScaler and Palo Alto Networks firewalls significantly reduce processing overhead on application and database servers and improves security.

The purpose of this guide is to help organizations deploy NetScaler and Palo Alto Networks next-generation firewalls for securing and load balancing Microsoft® Exchange 2010 Client Access servers. Inside this guide you will find a concise set of step-by-step deployment instructions required to configure both devices to accelerate and safely enable a Microsoft Exchange 2010 OWA application.

Within the Exchange 2010 server architecture, a NetScaler and next generation firewall is located in front of the Client Access Servers (CAS) with one single Virtual IP (VIP) address. The next-generation firewall secures the CAS systems and the NetScaler provides load balancing and traffic optimization. Exchange client traffic is bound to a Client Access Server through NetScaler. Each CAS system within the server pool handles the server applications, security, authentication, and connection and protocol processing. The Mailbox server at the back end handles the mailbox data, such as mail and contacts.

2. Requirements

<table>
<thead>
<tr>
<th>Required Component</th>
<th>Used in this Document</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix NetScaler</td>
<td>NS 10.0 VPX Build 69.4.nc with Platinum License</td>
<td></td>
</tr>
<tr>
<td>Palo Alto Networks Next-Generation Firewall</td>
<td>PAN-OS 4.1</td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange 2010 Servers</td>
<td>6 Physical/VM servers</td>
<td>2x CAS (Web); 1x Edge Transport; 1x Mailboxes; 1x Hub Transport; 1x AD</td>
</tr>
<tr>
<td>AppExpert Microsoft Outlook Web Access Template</td>
<td>Template File</td>
<td><a href="http://community.citrix.com/download/attachments/49186776/OWA.xml">http://community.citrix.com/download/attachments/49186776/OWA.xml</a></td>
</tr>
<tr>
<td></td>
<td>Deployment File</td>
<td><a href="http://community.citrix.com/download/attachments/49186776/OWA_deployment.xml">http://community.citrix.com/download/attachments/49186776/OWA_deployment.xml</a></td>
</tr>
</tbody>
</table>

3. Microsoft Exchange Server Network Topology

3.1 Environment diagram

![Diagram of Exchange Server Network Topology]

- Zone 1 – Front-End
- Zone 2 – DMZ
- Zone 3 – Back-End
- Zone 4 – Mid-tier
- Zone 5 – Infrastructure
### 3.2 IP allocations

<table>
<thead>
<tr>
<th>Functional Device</th>
<th>IP:Port</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler IP (NSIP)</td>
<td>10.5.172.124</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>NetScaler Subnet IP (SNIP)</td>
<td>10.5.172.126</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange OWA (VIP) – Web</td>
<td>10.5.172.165:443</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange OA (VIP) – Outlook</td>
<td>10.5.172.165:443</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange AS (VIP) – Mobile</td>
<td>10.5.172.165:443</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange IMAP4 – IMAP Client</td>
<td>10.5.172.165:993</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange POP3 – POP Client</td>
<td>10.5.172.165:995</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange SMAP Relay</td>
<td>10.5.172.166:25</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange CAS Server 1</td>
<td>10.5.172.160</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange CAS Server 2</td>
<td>10.5.172.161</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange ET Server</td>
<td>10.5.172.162</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange Mailbox Server</td>
<td>10.5.172.163</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Exchange HT Server</td>
<td>10.5.172.164</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Active Directory Server</td>
<td>10.5.172.155</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

### 4. Microsoft Exchange Installation and Configurations

The configuration of Citrix NetScaler for Microsoft Exchange 2010 is made up of 5 key steps:

1. Setup the underlying network
2. License the system
3. Configure the policies for Microsoft Exchange 2010
4. Setup SSL
5. Setup which servers will receive traffic from the NetScaler

The third step in particular is noteworthy. Traditionally, there are numerous policies that must be configured to correctly enable all of the features for optimal traffic management for Microsoft Exchange. Everything from traffic switching to optimization is affected in this step. With Citrix NetScaler, we are able to leverage the AppExpert AppTemplate for Microsoft Exchange 2010 which provides a single configuration file to load in order to get all of the correct settings configured. For additional AppExpert Templates for other applications, visit [http://community.citrix.com/display/ns/AppExpert+Templates](http://community.citrix.com/display/ns/AppExpert+Templates).

The AppExpert Templates published by Citrix do not contain certain application- and custom environment-specific parameter settings. Elements which are not predefined include IP addresses, number of servers, SSL parameters and others. Since the AppExpert Template for Exchange 2010 only supports Microsoft Outlook Web Access (OWA), there will be separate steps to manually configure the rest of Exchange services such as Outlook Anywhere (OA, i.e., Outlook client), ActiveSync (AS, i.e., mobile client), IMAP4, POP3 and external SMTP relay services. The following steps guide where and how each custom data will be added.
4.1 NetScaler Configuration

During the installation and configuration process, from the main NetScaler screen, administrators will be able to navigate the menu (in red) panel to configure application-specific parameters or to confirm the data already populated by the template.

The table below summarizes the specific menu and actions within NetScaler which need to be configured properly in order to complete the Exchange configuration:

<table>
<thead>
<tr>
<th>Service</th>
<th>NetScaler Menu</th>
<th>NetScaler Sub-Menu</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>System</td>
<td>Licenses</td>
<td>Manage Licenses</td>
<td>Custom added*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Settings</td>
<td>Configure basic features</td>
<td>Custom added*</td>
</tr>
<tr>
<td>All</td>
<td>Network</td>
<td>IPs</td>
<td>NetScaler IP, Subnet IP</td>
<td>Custom added*</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Virtual IP</td>
<td>Auto added **</td>
</tr>
<tr>
<td>All</td>
<td>SSL</td>
<td>Certificate</td>
<td>Root-CA, Server</td>
<td>Custom added*</td>
</tr>
<tr>
<td>All</td>
<td>SSL Offload</td>
<td>Servers</td>
<td>Per VM/Physical Server</td>
<td>Auto added</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service Group</td>
<td>Per Port</td>
<td>Auto added</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virtual Servers</td>
<td>VIP per Port</td>
<td>Auto added</td>
</tr>
<tr>
<td>OWA</td>
<td>AppExpert</td>
<td>Applications</td>
<td>Import</td>
<td>Custom added*</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configure Public</td>
<td>Custom</td>
</tr>
</tbody>
</table>
**Endpoints added**

<table>
<thead>
<tr>
<th>Service</th>
<th>Load Balancing</th>
<th>Virtual Servers</th>
<th>VIP per Port</th>
<th>Custom added*</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OWA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Group</th>
<th>Per Port</th>
<th>Custom added*</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Service Groups added**

<table>
<thead>
<tr>
<th>Service Groups</th>
<th>Per Port</th>
<th>Custom added*</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Virtual Servers added**

<table>
<thead>
<tr>
<th>Virtual Servers</th>
<th>VIP per Port</th>
<th>Custom added*</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Servers added**

<table>
<thead>
<tr>
<th>Servers</th>
<th>Per VM/Physical Server</th>
<th>Auto added</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Please refer below 4.2 Step-by-step Installation for custom environment setup
** Auto added – The data will be populated automatically when the template is installed and 'Custom added' data is added (Please do not modify manually 'Auto added' data)
*** Auto added – The Exchange environment in this deployment doc shares the same CAS servers for OA/AS services with OWA, and sharing same port numbers. Therefore, no additional service configuration is required.

## 4.2 Step –by-Step Installation

The following steps are required to get the downloaded Exchange AppExpert template installed and operational.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Detail</th>
<th>Custom Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NetScaler IP, Subnet IP</td>
<td>NetScaler initial Configuration (by Setup Wizard)</td>
<td>NetScaler IP (NSIP), Subnet IP (SNIP)</td>
</tr>
<tr>
<td>2</td>
<td>Manage Licenses</td>
<td>NetScaler license installation</td>
<td>.lic license file</td>
</tr>
<tr>
<td>3</td>
<td>Configure basic features</td>
<td>NetScaler basic feature settings</td>
<td>Feature settings</td>
</tr>
<tr>
<td>4</td>
<td>Import</td>
<td>Template Import</td>
<td>Template, Deployment files (XML format)</td>
</tr>
<tr>
<td>5</td>
<td>Root-CA, Server</td>
<td>Security Certificate Installation</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Configure Public Endpoints</td>
<td>Creating virtual servers (IP) to talk to multiple backend servers</td>
<td>OWA Virtual IP (VIP)</td>
</tr>
<tr>
<td>7</td>
<td>Configure Backend Services</td>
<td>Creating a Service Group</td>
<td>IPs for Web Server 1 and Web Server 2</td>
</tr>
<tr>
<td>8</td>
<td>Per Port, VIP/Port</td>
<td>IMAP4 Service Installation</td>
<td>IMAP4 port</td>
</tr>
</tbody>
</table>
5. Deployment Instructions

This section will describe details of the NetScaler VPX installation and initial configuration, Exchange AppExpert template download, and full SharePoint service configuration within NetScaler. Administrators can use the NetScaler command-line to set up the initial NSIP, Mapped IP (MIP), and Subnet IP (SNIP). Administrators can also configure advanced network settings and change the time zone.

For information about MIP, SNIP, other NetScaler-owned IP addresses, and network settings, see the “Citrix NetScaler Networking Guide” at http://support.citrix.com/article/CTX132369.

5.1.1 Add NSIP, Subnet Mask, and Default Gateway on NetScaler:

At the Console prompt from XenCenter or vSphere client, enter the NSIP address, subnet mask, and then save the configuration. Use either the SSH client or the NetScaler VPX Console to access the NetScaler command line to complete initial configuration with default gateway.

`> add route 0.0.0.0 0.0.0.0 <gateway ip>
> show route
> save ns config`

5.1.2 NetScaler Configuration by Using the Configuration Utility

Once the network connectivity to NetScaler is established, the Configuration Utility can be accessed from a browser to complete the rest of the Microsoft Exchange configuration. Connect to NetScaler on a web browser: http://<NSIP address>. In Start in, select Configuration, and then click Login. Setup Wizard should start up automatically. Otherwise, Setup Wizard can be started from menu under Netscaler>System Information:
5.1.3 Setup Wizard

Click **Next** to follow the instructions. Confirm the pre-populated **NSIP**, **Netmask** and **Gateway** addresses.
Choose **Subnet IP (SNIP)** to add SNIP address and its subnet mask (Netmask) and Click **Next**.

Choose **Skip this Step** for now. AppExpert Template can be added in another step.
5.2 NetScaler License installation

Proper licenses are required in order to enable necessary services for the Exchange configuration. Refer to the "Citrix NetScaler VPX Licensing Guide" at [http://support.citrix.com/article/CTX122426](http://support.citrix.com/article/CTX122426).

Click **Manage License** to install the downloaded license.

Click here to request for licenses.
5.3 NetScaler Basic Feature Setting

5.3.1 Systems Settings

Once a proper license is installed, administrator can select the available features to enable them from **Systems>Settings.** Choose **Configure basic features.**

5.3.2 Basic Features

The following services are the minimal services required in order to enable and complete the Exchange configuration.
5.4 NetScaler AppExpert Outlook Web Access Template Install

AppExpert Outlook Web Access template can be imported under AppExpert navigation panel then choose Import AppExpert Template.
Click **Next** to bring **AppExpert Template Wizard** to upload the downloaded templates.

Choose **Browse (Local)** if the files were downloaded to local system, then choose the proper **Template** and **Deployment** files for Exchange. Then, click **Next**.
AppExpert Template Wizard will confirm with the Name then click Finish to complete.

If any of required services for OWA were not enabled, the following Warning will guide through to enable those features. Click Yes.

By default, the memory usage limit was set to 0. Proceed message will prompt to change the value of memory limit parameter. Click Yes.

Set Memory Usage Limit (MB) to 300. Then click OK.
Confirm enabled **Basic Features.** Click **OK.**
5.5 NetScaler SSL Security Certificate installation (Self-Signed Certificate example)

If production certificates are available, these can be imported through the processes within the NetScaler management interface. Consult Chapter 11, “Securing Load Balanced Traffic by Using SSL” of the NetScaler product documentation entitled “NetScaler VPX Getting Started Guide” for details pertaining to the user of existing certificate/key pairs.

The following steps were used in this reference environment to create of self-signed certificates used to implement the HTTP to HTTPS rewrite.

5.5.1 Root-CA Certificate

Under SSL navigation panel, choose Root-CA Certificate Wizard.
Click Next.

Set the Key Filename to Exchange-CA-Key. And set Key Size to 1024 or any value that reflects customized datacenter’s standard. Then click Next.
Set the **Request File Name** to **Exchange-CA-CSR**. And set **City** and **State or Province**, **Organization Name** to appropriate values. Then click **Next**.

Set the **Certificate File Name** to **Exchange-CA-Certificate**. Then click **Next**.
Set the **Certificate-Key Pair Name** to **Exchange-CA-CertKey**. Then click **Next**.

**Certificate Wizard**

**Install Certificate**
Add a certificate-key pair object.

- **Certificate-Key Pair Name**: Exchange-CA-CertKey
- **Certificate File Name**: Exchange-CA-Certificate
- **Private Key File Name**: Exchange-CA-Key
- **Password**: 
- **Certificate Format**: ○ PEM ○ DER

**Details**
Certificate and key files are stored in the folder /nsconfig/ssl/ on appliance.

**Notify When Expires** ○ Enable ○ Disable
**Notification Period** 

Click **Finish** then **Exit**.
5.5.2 Server Certificate

Under SSL navigation panel, choose Server Certificate Wizard.

Click Next.
Set the **Key Filename** to **Exchange-Server-Key**. And set **Key Size** to 1024 or any value that reflects customized datacenter’s standard. Then click **Next**.

Set the **Request File Name** to **Exchange-Server-CSR**. And set **City** and **State** or **Province**, **Organization Name** to appropriate values. Then click **Next**.
Set the **Certificate File Name** to **Exchange-Server-Certificate**. And set **CA Certificate File Name** to **Exchange-CA-Certificate**. Set **CA Key File Name** to **Exchange-CA-Key**. And **CA Serial Number File** to **CAExchange**. Then click **Next**.

Set the **Certificate-Key Pair Name** to **Exchange-Server-CertKey**. Then click **Next**.
Click Finish.

You specified the following configuration settings:

- Key File: Exchange-Server-Key
- Certificate Request File: Exchange-Server-CSR
- Certificate Key pair name: Exchange-Server-CertKey

To make any changes, click Back.
To complete the configuration, click Finish.

Click Exit.

The configuration is successful.
Click Exit to close the wizard.
5.6 Creating virtual servers (VIP)

Virtual servers (or Virtual IP, VIP) will be used for users to connect to Exchange service. Once completed, users will be able to access their SharePoint environment to [http(s)://<VIP>] or [http(s)://<VIP>/owa] depending on their configuration.

5.6.1 HTTP VIP

Under AppExpert navigation panel, choose Applications to view those installed templates. Under OWA, all the pre-defined Exchange service components will be listed. Choose Configure Public Endpoints… to set public virtual server name and ip address according to section 3.2.

Choose Add.

Choose Public Endpoints (OWA)

Activate All  Deactivate All

<table>
<thead>
<tr>
<th>Active</th>
<th>Name</th>
<th>IP Address</th>
<th>Port</th>
<th>Proto...</th>
<th>State</th>
</tr>
</thead>
</table>

Add...  Open...  Remove

Help

OK  Close
Set **Name**, **IP Address**, **Port**, and **Protocol**. Click **Create**.

Set **Persistence Time-out (min)** to 2. Then click **OK**.
5.6.2 HTTPS VIP

From the main NetScaler Configuration Utility screen, under AppExpert and Applications, and OWA, choose Configure Public Endpoints… to set public virtual server name and ip address according to section 3.2. (Note. This IP address will be the same as HTTP VIP which was just created in previous section. It will just use a different port.). Set Name to CASFe_FE_SSL or meaningful name. Set IP Address, Port 443 and Protocol as HTTPS. Then click Create.

Highlight CAS_FE_SSL then click Open…
Set Persistence Time-out (min) to 2. Click SSL Settings.

Choose the Certificates which were created in previous section 5.5. Click the arrow button under Add> to choose as CA> to add CA CertKey.
Click OK.
5.7 Creating a Service Group

From the main NetScaler Configuration Utility screen, under AppExpert and Applications, and OWA, choose Configure Backend Services… to set Service Groups to add physical/VM server IP addresses.

Click Add…

Configure Backend Services

<table>
<thead>
<tr>
<th>Services</th>
<th>Service Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate All</td>
<td>Deactivate All</td>
</tr>
<tr>
<td>Active</td>
<td>Service Group Name</td>
</tr>
<tr>
<td>✔</td>
<td>CAS Servers-SSL</td>
</tr>
<tr>
<td></td>
<td>SharePoint Servers</td>
</tr>
<tr>
<td></td>
<td>CAS Servers</td>
</tr>
</tbody>
</table>
Set **Service Group Name** to **CASServers-SSL** or proper meaningful name. Set **IP address** under **Specify Member(s)**. Then **Add**.

Choose **Monitor**. Then add **http-env**.
Select CASServers-SSL which was just created under Configure Backend Services.

Choose **Method and Persistence** to set **Round Robin** under **Method**. And set **Persistence** to **SSLSESSION**.
5.8 IMAP4 installation

IMAP4 service was not added as part of Exchange (OWA) AppExpert Template. In order to install and configure the service, a service group needs to be created with physical/VM servers to be load balanced. Then a virtual server will be created using the service group.

From main NetScaler navigation panel, choose Service Groups under Load Balancing. Click Add...

Set Service Group Name to Exchange_IMAP4 and add designated physical/VM servers under Specify Members(s) with 993 Port. Click Create.
Under Load Balancing navigation panel, choose Virtual Servers. Click Add…

Set Name to Exchange_IMAP4_VIP and IP Address. Protocol to SSL_TCP. Choose Method and Persistence tab. Set Round Robin Method and SSLSESSION Persistence.

Binding Exchange_IMAP4 service group under Service Groups tab.
Add **Certificates** under SSL Settings. Then click **Create**.

### 5.9 POP3 installation

POP3 service was not added as part of Exchange (OWA) AppExpert Template. In order to install and configure the service, a *service group* needs to be created with physical/VM servers to be load balanced. Then a *virtual server* will be created using the *service group*. 
From main NetScaler navigation panel, choose **Service Groups** under **Load Balancing**. Click Add...

Set **Service Group Name** to **Exchange_POP3** and add designated physical/VM servers under **Specify Members(s)** with 110 Port. Click **Create**.
Under **Load Balancing** navigation panel, choose **Virtual Servers**. Click **Add**...

Set **Name** to *Exchange_POP3_VIP* and **IP Address**. **Protocol** to *SSL_TCP*. Choose **Method and Persistence** tab. Set **Round Robin** Method and **SSLSESSION Persistence**. Binding *Exchange_POP3* service group under **Service Groups** tab.
Add Certificates under SSL Settings. Then click Create.
5.10 SMTP installation

SMTP service was not added as part of Exchange (OWA) AppExpert Template. In order to install and configure the service, a service group needs to be created with physical/VM servers to be load balanced. Then a virtual server will be created using the service group.

From main NetScaler navigation panel, choose Service Groups under Load Balancing. Click Add…
Set **Service Group Name** to **Exchange_SMTP** and add designated physical/VM servers under **Specify Members(s)** with 25 Port. Click **Create**.

Under **Load Balancing** navigation panel, choose **Virtual Servers**. Click **Add**...

Set **Name** to **Exchange_SMTP_VIP** and **IP Address**, **Protocol** to **TCP**. Choose **Method and Persistence** tab. Set **Round Robin** Method and **SSLSESSION** Persistence. Binding **Exchange_SMTP** service group under **Service Groups** tab.
5.11 Outlook Anywhere, ActiveSync confirmation

Microsoft Outlook Anywhere (OA) allows Exchange access through the Microsoft Outlook client by tunneling Outlook’s MAPI protocol over an HTTP connection. Microsoft Exchange ActiveSync (AS) client synchronizes data between mobile devices and Exchange 2010. E-mail, contacts, calendar information, and tasks can be synchronized over an HTTP connection.

Since OA and AS services are connecting to Exchange servers over secured SSL (443) tunneling to an HTTP (80) connection which is the same way Outlook Web App (OWA) does, if Client Access Server (CAS) was set up as a multi-mode service including OWA, OA and AS, then there won’t be any necessary service configuration for OA and AS. If OA and AS are serviced in a separated server from OWA, the configuration steps will be the same as OWA in previous chapter 5.

6. Services Verifications

As described in section 4.1, some required configuration will be added automatically as part of installation and configuration of ‘Custom added’ data. Once all the data is installed and configured properly in chapter 5, administrators should be able to confirm and verify other data (‘Auto added’) which were added automatically.

6.1 Network IPs and Virtual IPs

NetScaler IP, Subnet IP and Virtual IP can be found under Network>IPs>IPV4s:
6.2 SSL Offload – Servers, Service Groups

Under SSL Offload, Backend Servers which were created with Backend Service Group can be found under Servers:
Under **SSL Offload**, *Backend Server Group* which was created can be found under *Service Groups*:

Under **SSL Offload**, *public endpoints* which were created can be found under *Virtual Servers*:
6.3 Load Balancing – Servers, Service Group

Under **Load Balancing**, **Servers** and **Service Groups** can be confirmed:
6.4 Content Switching

AppExpert Template uses **Content Switching** to add its virtual server. Under **Content Switching**, **Virtual Servers** can be found:
7. Monitoring – NetScaler Dashboard

NetScaler provides Dashboard to display System Overviews, Logs, and Service Summary per Service Group(s):

7.1 By Service Groups

Under CAServers-SSL , Exchange_IMAP4, Exchange_POP3, and Exchange_SMTP service groups -
7.2 Per Server

Under **Service Group Member Summary**, service details including # of Requests, Responses can be found:
8. Palo Alto Networks Next-Generation Firewall Deployment

The Palo Alto Networks next-generation firewall safely enables enterprise applications in the data center and delivers meaningful segmentation by application, user and content. It identifies all traffic sent to the Microsoft Exchange servers, based on actual application, not just port or protocol. Access to the Microsoft Exchange servers can be further restricted to only the authorized users or groups. All content is scanned for malicious content - viruses, malware, and spyware – and dropped before they can reach the data center servers.

8.1 Data Center Segmentation

In an Exchange data center implementation, there will be several different roles performed by the servers. In smaller implementations, some of these roles can be combined in a single server. For large Exchange installations, the different server roles will be deployed on dedicated physical or virtual servers.

In order to properly segment and secure a large Exchange implementation, the different server roles will be isolated in dedicated security zones that can only be accessed by authorized users with authorized applications.

In this reference design, there will be segments for the Exchange Client Access Servers, Edge Transport Servers, Hub Transport Servers, and Mailbox Servers. Users and administrators accessing the Exchange servers will come from the External zone, and there will be an infrastructure segment in which the Active Directory Domain Controllers reside.

To build these segments in the Palo Alto Networks firewall, the following zones will be created:

- **Web** – Exchange Client Access Servers
- **DMZ** – Edge Transport Servers
**Application** – Hub Transport Servers

**Database** – Mailbox Servers

**Active-Directory** – Domain controller

**External** – Users and administrators

For example, to create the Web zone, go to the Network tab, under the Zone section and click Add.

Enter the name of the zone, the type – Layer2 or Layer3, and click the check box for Enable User Identification.

Repeat this for each of the required zones.

---

### 8.2 Security Policy

The Palo Alto Networks next-generation firewall security policy is zone-based. Each segment in a data center deployment will be in a separate zone. Once the traffic flow is understood, the security policy can be written based on actual application, not just ports and port ranges. Allowing the following protocols between the specified zones will enable Exchange, while restricting non-Exchange traffic.

Every Exchange implementation is different, and depending on the features and services enabled, the specific applications between zones, as well as the required zones, may vary. This will serve as a starting reference for a working Exchange security policy.

<table>
<thead>
<tr>
<th>Source Zone</th>
<th>Destination Zone</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active-Directory</td>
<td>DMZ</td>
<td>netbios-ns</td>
</tr>
<tr>
<td>Active-Directory</td>
<td>External</td>
<td>dns</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>-----</td>
</tr>
<tr>
<td>Active-Directory</td>
<td>Web</td>
<td>ms-ds-smb msrpc netbios-dg netbios-ns netbios-ss</td>
</tr>
<tr>
<td>Application</td>
<td>Active-Directory</td>
<td>dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss rpc</td>
</tr>
<tr>
<td>Application</td>
<td>Database</td>
<td>ms-ds-smb msrpc netbios-dg netbios-ss</td>
</tr>
<tr>
<td>Application</td>
<td>External</td>
<td>dns kerberos rpc</td>
</tr>
<tr>
<td>Database</td>
<td>Active-Directory</td>
<td>active-directory dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss rpc</td>
</tr>
<tr>
<td>Database</td>
<td>Application</td>
<td>ms-ds-smb msrpc netbios-dg netbios-ss</td>
</tr>
<tr>
<td>Database</td>
<td>External</td>
<td>web-browsing</td>
</tr>
<tr>
<td>DMZ</td>
<td>Active-Directory</td>
<td>dns ldap ms-ds-smb netbios-dg netbios-ss</td>
</tr>
<tr>
<td>DMZ</td>
<td>External</td>
<td>web-browsing</td>
</tr>
<tr>
<td>External</td>
<td>Active-Directory</td>
<td>active-directory dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss rpc</td>
</tr>
<tr>
<td>External</td>
<td>Application</td>
<td>smtp</td>
</tr>
<tr>
<td>Source Zone</td>
<td>Destination Zone</td>
<td>Services</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------</td>
<td>----------</td>
</tr>
<tr>
<td>External</td>
<td>Web</td>
<td>imap, ms-ds-smb, ms-exchange, msrpc, netbios-dg, netbios-ss, outlook-web, pop3, rpc-over-http, ssl, web-browsing</td>
</tr>
<tr>
<td>Web</td>
<td>Active-Directory</td>
<td>active-directory, dns, kerberos, ldap, ms-ds-smb, ms-netlogon, msrpc, netbios-dg, netbios-ss, rpc</td>
</tr>
<tr>
<td>Web</td>
<td>Application</td>
<td>ms-ds-smb, msrpc, netbios-dg, netbios-ss</td>
</tr>
<tr>
<td>Web</td>
<td>Database</td>
<td>ms-ds-smb, msrpc, ms-exchange, netbios-dg, netbios-ss, rpc-over-http, ssl, web-browsing</td>
</tr>
<tr>
<td>Web</td>
<td>External</td>
<td>active-directory, dns, kerberos, ldap, ms-ds-smb, ms-netlogon, msrpc, netbios-dg, netbios-ss, rpc, web-browsing</td>
</tr>
</tbody>
</table>

To create the security policy, each of these source and destination zone pairs will represent one rule in the security policy. For example, to create the “Application to Database” security policy, on the Palo Alto Networks firewall, go to the Policies tab (on top), and the Security section (on left), and click Add (on bottom). Enter the name of the security policy rule.
Click on the Source tab and click Add. Select the Application zone.
Click on the Destination tab and click Add. Select the Database zone.

Click on the Application tab and click Add. Four applications will be added to this rule: ms-ds-smb, msrpc, netbios-dg, and netbios-ss. Begin typing the first application name and select it when it appears in the list.
Repeat for the remaining applications in this rule.

Click OK. The rule will be added to the security policy. Repeat this process for each of the source and destination zone pairs listed above.
8.3 User Identification

The Palo Alto Networks firewall also allows security policy to be further refined by end user or group, not just source IP. Certain servers, or certain applications in the data center may only need to be accessed by specific people or groups. The next-generation firewall will retrieve user and group information from the local user directory service, and allow that information to be used in security policies.

For example, the Exchange servers may need to be accessible by system administrators with Remote Desktop for management purposes. But, other users do not need this access. The security policy rule allowing the applications, in this case, ms-rdp and t.120, would only be accessible by the administrators group. Exchange would be accessible by other users using the client applications.

8.4 Threat Protection

In addition to validating the application used to access a security zone and the user initiating the request, the next-generation firewall can scan the network traffic for known and unknown threats. These include viruses, malware, spyware, or files with confidential data. By creating a security profile that scans traffic into the data center, the firewall can prevent a user from unknowingly infecting data center servers with malware, or getting infected from a compromised server.

Each rule in the security policy can have its own security profile applied, allowing for the greatest flexibility in setting policy. For example, you may have a strict security profile blocking viruses, malware, and spyware on traffic that originates outside the data center and accesses the front-end servers, but not have any inspection on traffic between the application and database servers.

To begin creating the security profile, locate the Profile column in the security policy page. If nothing has been configured there yet, it will indicate “none”.
Click the “none” and a dialog window will open. Choose “Profiles” from this window to configure the security profile.
In the security profile window, select the specific profile settings for each of the different areas, Antivirus, Vulnerability Protection, etc. Some of these will have pre-configured profiles, such as “default” or “strict”. These pre-configured options can be chosen, or a customized profile can be created. Please see Palo Alto Networks Administration Guide for details on creating custom profiles.

Click OK, and the new security profile should now be part of the security policy rule. This will be displayed with icons for the specific areas that profiles were chosen for.
Repeat this process for all of the rules that a security profile should be applied to.

9. References

Application Template Deployment Guide. Microsoft OWA. Citrix Systems, Inc. 2008
About Palo Alto Networks

Palo Alto Networks™ is the network security company. Its innovative platform allows enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks. The core of Palo Alto Networks’ platform is its Next-Generation Firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks’ products and services can address a broad range of network security requirements, from the data center to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices. Palo Alto Networks’ products are used by more than 9,000 customers in over 100 countries. For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, “The Network Security Company,” the Palo Alto Networks Logo, App-ID, GlobalProtect, and WildFire are trademarks of Palo Alto Networks, Inc. in the United States. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners.

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) transforms how businesses and IT work and people collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 organizations. Citrix products touch 75 percent of Internet users each day and it partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com.

©2012 Citrix Systems, Inc. All rights reserved. Citrix® and NetScaler® are trademarks or registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.