Virtual Systems

Using and Configuring Palo Alto Networks Virtual Systems Functionality with PAN-OS 4.1

April 2012

Palo Alto Networks
3300 Olcott Street
Santa Clara, CA 94054
www.paloaltonetworks.com

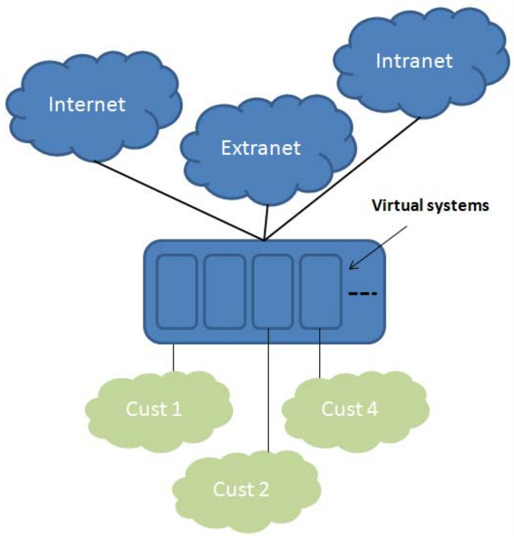
Table of Contents

EXECUTIVE SUMMARY

This document is divided into two sections. The first section provides an overview of the Palo Alto Networks virtual systems functionality, including a brief description of deployment scenarios. The second section will provide some technical details on how a virtual system is configured.

OVERVIEW

Virtual systems (vsys) are unique and distinct next-generation firewall instances within a single Palo Alto Networks firewall. Rather than deploy many individual firewalls, managed service providers and enterprises can deploy a single pair of firewalls (high availability) and enable a series of virtual firewall instances or virtual systems. Each vsys is an independent (virtual) firewall that is managed separately and cannot be accessed or viewed by any other user.



Centralized management combined with role based administration means that the administrator can control access to the device level as well as specific management functions (enable, disable, hide) for each firewall customer or user. The flexibility and efficiencies of virtual systems present managed service providers (MSP) and enterprises with some very attractive possibilities to enhance business efficiencies:

- **Improved scalability:** Once the initial physical firewall is deployed, adding or removing customers or business groups can be done quickly and efficiently. A managed service provider can offer differentiated security services for each of his customers while keeping the cost and complexity down by operating from a simplified infrastructure. A large enterprise can use virtual systems to provide next-generation firewall protection for business groups, departments, or subsidiaries.
- **Lower capital expenditures:** Using a single physical firewall to support multiple, distinct customers or business units is more cost effective then buying and deploying many physical firewalls.
- **Reduced operational expenditures:** Fewer physical firewalls will consume smaller amounts of rack space, fewer BTUs and less electricity. Management costs will also be reduced, again, because there are fewer physical instances to manage.

Each Palo Alto Networks virtual system provides all of the same basic functionality that a unique physical device supports, allowing an organization to take a menu-based approach to security services delivery.

The table below outlines the key functionality that is available in both a physical device and a virtual system.

Supported Functionality	Physical Appliance	Virtual Systems
Application visibility and control (App-ID)	Yes	Yes
SSL decryption and inspection (App-ID)	Yes	Yes
SSH control (App-ID)	Yes	Yes
Custom App-ID	Yes	Yes
User-based control – Active Directory, LDAP, eDirectory Microsoft Exchange (User-ID)	Yes	Yes
User-based control – Citrix and Terminal services (User-ID)	Yes	Yes
User-based control – Captive portal (User-ID)	Yes	Yes
Customized user-based control – XML API (User-ID)	Yes	Yes
Vulnerability protection (Content-ID)	Yes	Yes
Virus protection (Content-ID)	Yes	Yes
Spyware protection (Content-ID)	Yes	Yes
URL filtering (Content-ID)	Yes	Yes
WildFire	Yes	Yes
Data filtering	Yes	Yes
File blocking	Yes	Yes
QoS	Yes	Yes
IPSec VPN (site-to-site)	Yes	Yes
SSL VPN (remote user access)	Yes	Yes
GlobalProtect	Yes	Yes
Logging and reporting	Yes	Yes
Centralized management	Yes	Yes
Role based administration	Yes	Yes
Network segmentation (security zones, VLANs, virtual routers)	Yes	Yes
Routing and switching (BGP, OSPF, RIP, L2, L3, mixed mode, virtual wire)	Yes	Yes
High Availability (Active/passive, Active/active)	Yes	Yes

VIRTUAL SYSTEMS DEPLOYMENT SCENARIOS

There are many ways in which virtual systems can be used, however the most common are either as a means of managed services delivery or within a large enterprise where the technical requirements dictate separate firewall instances, each with their own unique firewall configuration.

- **Managed services:** Within a managed services environment, the cost effectiveness of a single device supporting distinct firewall instances can help improve the bottom line by allowing the provider to deliver security services to multiple customers with a single device. The breadth of functionality and the configuration flexibility would allow each customer to select from a menu of service offerings, each of which can be enabled and disabled quickly and effectively. Role-based administration would allow the service provider to enable the end customer to have access to certain functions (such as logging and reporting) while hiding or providing read-only (policy editor) access to other functions.

- **Departmental services**: In some large organizations certain technical or compliance requirements may dictate that departmental traffic be protected by a unique firewall instance. On an internal network, a single firewall instance with virtual systems support may be a cost effective solution. In this scenario, each department may be assigned security services from the "menu" and then billed back for those services to demonstrate a return on investment.

Just as with a managed services environment, department personnel can be allowed to have either read only or full access to certain firewall functions while the device itself is managed centrally by IT.

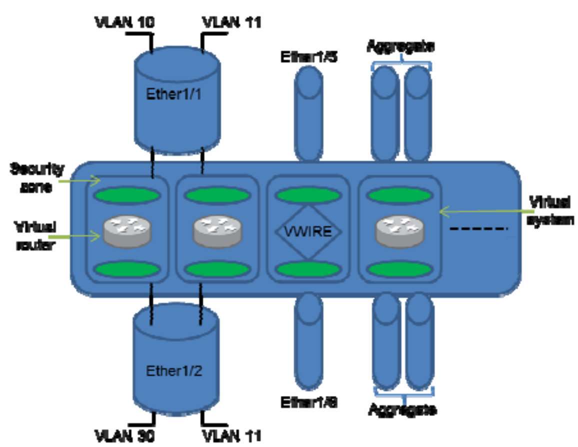
PLATFORM SUPPORT

Virtual systems are available on the PA-5000 Series, PA-4000 Series and the PA-2000 Series.

Platform	Base quantity virtual systems	Add-on virtual systems via license	Maximum virtual systems
PA-5060	25	200	225
PA-5050	25	100	125
PA-5020	10	10	20
PA-4060	25	100	125
PA-4050	25	100	125
PA-4020	10	10	20
PA-2050	1	5	6
PA-2020	1	5	6
PA-500	Not Available	Not Available	Not Available
PA-200	Not Available	Not Available	Not Available

ACCESSING VIRTUAL SYSTEMS

Traffic from different customers or departments can be directed to a virtual system using one of several mechanisms as shown in the diagram below. In virtual wire deployments, traffic passing between a pair of physical interfaces is directed to a particular virtual system. In layer 2 and layer 3 deployments, traffic may be differentially associated with a virtual system based on its VLAN tag. Note that all of the access methods described can be used concurrently on the firewall. A deployment mode (virtual wire, L2 and L3) for a specific virtual system can be selected independently for each virtual system.



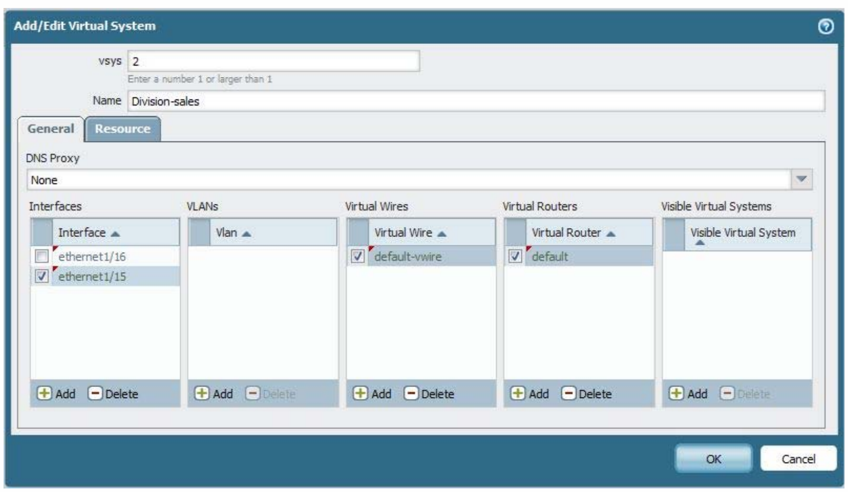
DEFINING VIRTUAL SYSTEMS

Interfaces and security zones can be grouped into virtual systems, and then managed independently of each other. For example, if you define virtual systems for the interfaces associated with specific departments or customers, you can then customize the administrative access, security policies, and logging/reporting for each department or customer.

You can also define administrator accounts that provide administrative or view-only access to a single virtual system. Initially, all interfaces, zones, and policies belong to the default virtual system (vsys1). When you enable multiple virtual systems, note the following:

- Interfaces, zones, VLANs, virtual wires, and virtual routers (VR) must be assigned to a virtual system (a virtual system column is added to the respective pages).
- A virtual system drop-down list is added under the Policies and Objects tabs. Before defining a policy or policy object, you must select the appropriate virtual system.
- Remote logging destinations (SNMP, Syslog, and email), as well as applications, services, and profiles, can be shared by all virtual systems or limited to a selected virtual system.
- Virtual router(s), security zone(s) and VLAN(s) can be defined before creating the vsys or can be added in a later stage by specifying the vsys when the resource is created.

Before configuring virtual systems, they will need to be activated. Activation is done under the device tab from the Setup > Management tab > General settings page. Once the virtual systems feature is enabled, 'virtual systems' and 'shared gateway' menu items become available in the left tree menu under the device tab. A minimum amount of information is required to begin configuring the first virtual system. Note that vsys1 is the default virtual system which is always present.

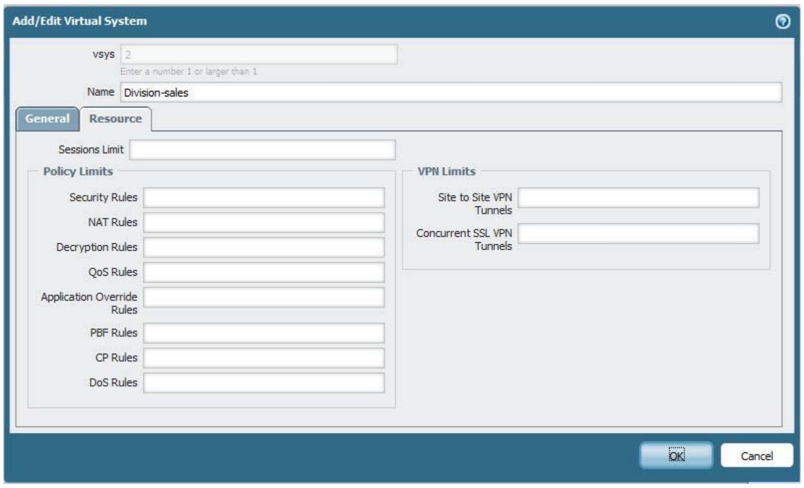


Virtual system resources can be limited per vsys through the 'Resource' tab.

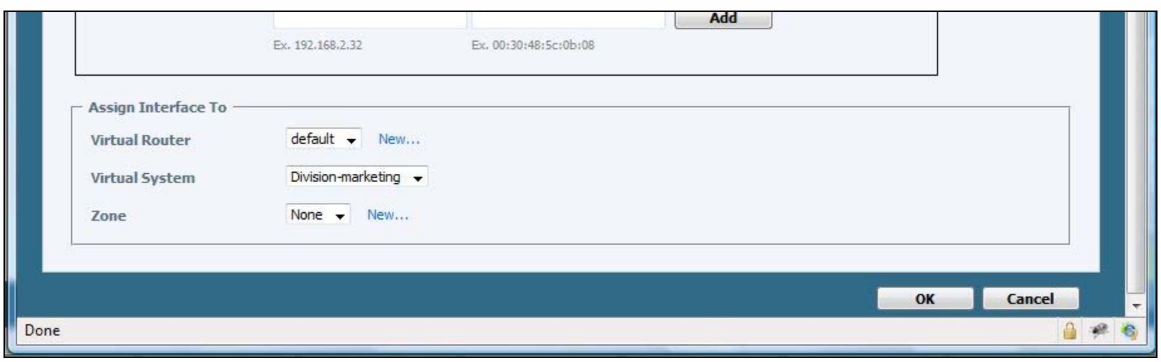
- **Sessions Limit**—Maximum number of sessions allowed for this virtual system.
- **Security Rules**—Maximum number of security rules allowed for this virtual system.
- **NAT Rules**—Maximum number of NAT rules allowed for this virtual system.
- **Decryption Rules**—Maximum number decryption rules allowed for this virtual system.
- **QoS Rules**—Maximum number of QoS rules allowed for this virtual system.
- **Application Override Rules**—Maximum number of application override rules allowed for this virtual system.
- **Policy-based Forwarding (PBF) Rules**—Maximum number of policy-based forwarding (PBF) rules allowed for this virtual system.
- **Captive Portal (CP) Rules**—Maximum number of captive portal (CP) rules allowed for this virtual system.

- **DoS Rules** —Maximum number of denial of service (DoS) protection rules allowed for this virtual system.
- **Site-to-Site VPN Tunnels**—Maximum number of site-to-site VPN tunnels allowed for this virtual system.
- **Concurrent SSL-VPN Tunnels**—Maximum number of concurrent SSL-VPN tunnels allowed for this virtual system.

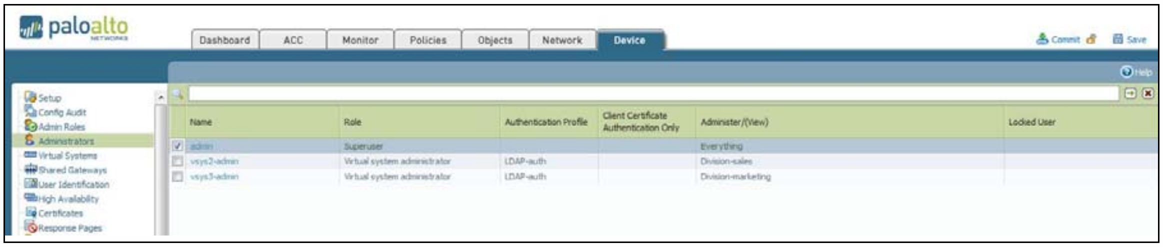
Per virtual system control helps ensure that the system resources are used efficiently and effectively. The image below shows the virtual system resource control.



The next step is to add the access interfaces/method to vsys2. In this example a layer 3 interface is added using a VLAN tag to classify the data. The trunk port can be shared by multiple virtual systems. Using a trunk port to service multiple virtual systems is a common technique.



If the virtual system needs to be managed by the customer or department, an administrator account will be required that is dedicated to the virtual system. The administrator may only change the objects and policies that are stored as part of that specific virtual system. A virtual system administrator does not have permissions to make changes to device-level constructs such as interfaces, virtual systems, and the contents of the Device tab in the web interface.

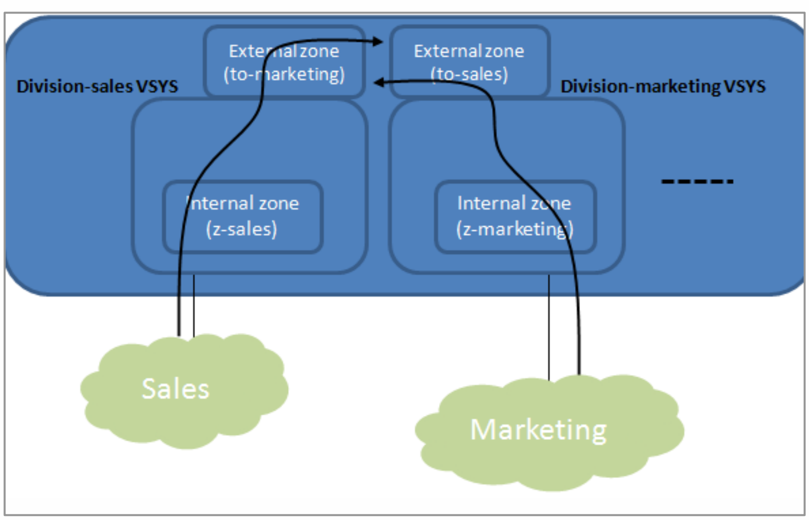


The default administrator (admin) can define policies and add security profiles (URL filtering, AV scanning, malware (IPS) scanning and Spyware/Adware scanning in addition to data leakage prevention (DLP)) to specific virtual systems.

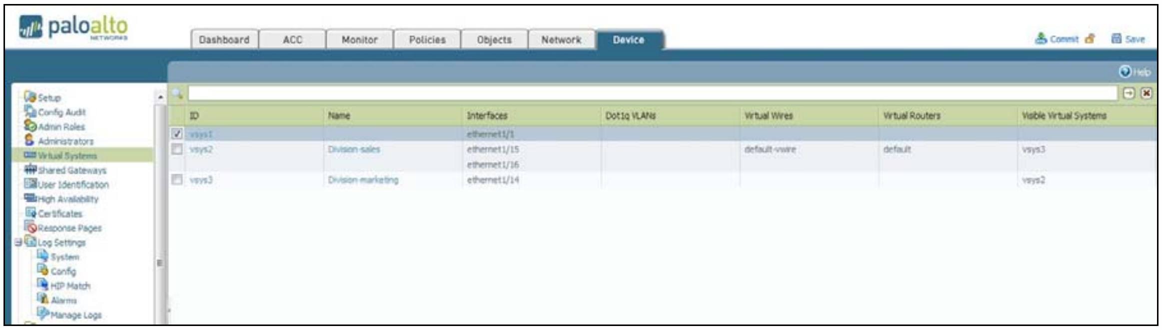
The dedicated virtual system administrator will only have a view of his own policy rule base.

DEFINING INTER-VSYS POLICIES

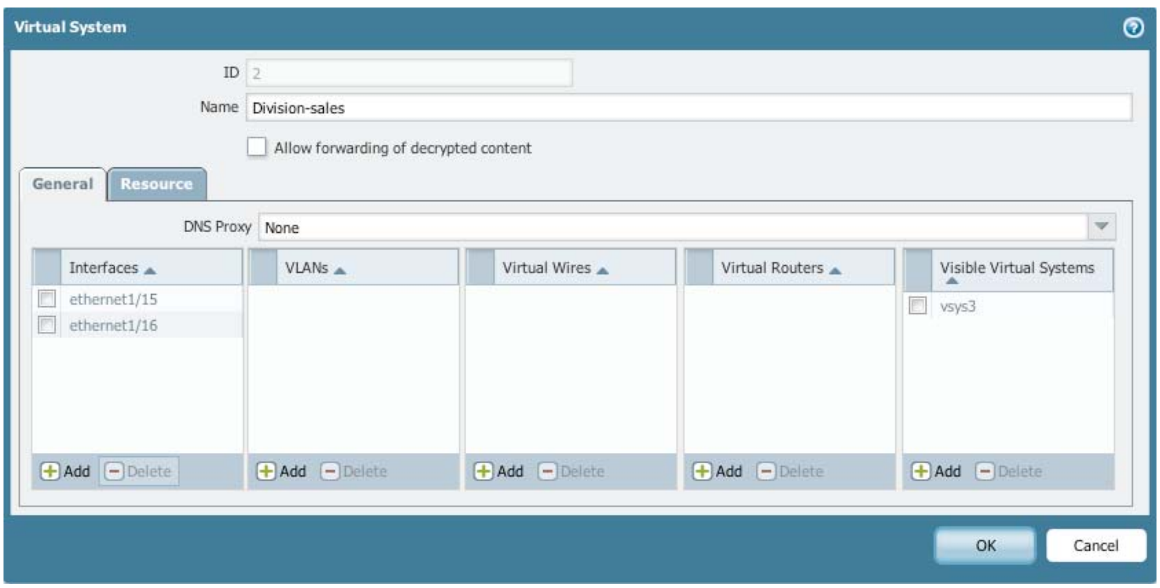
Inter-vsys traffic, also known as 'shared-vsys', allows the administrator to define systems where flows can traverse two vsys's without the need to leave the firewall when being routed between the vsys'. This type of vsys communication is beneficial for inter-departmental communication where there is a need for separate administrative domains. Inter-virtual system communication requires that the ingress and egress interfaces on the firewall be attached to a common virtual router, or be connected using inter-VR routing. Communication between virtual systems is controlled by security policies pointing to and from an 'external' vsys security zone. In this type of setup each of the vsys administrators will need to add the required policies to permit sessions between the two vsys'.In the example below vsys#2 (Division-Sales) needs to communicate with vsys#3 (Division-Marketing) through the firewall.



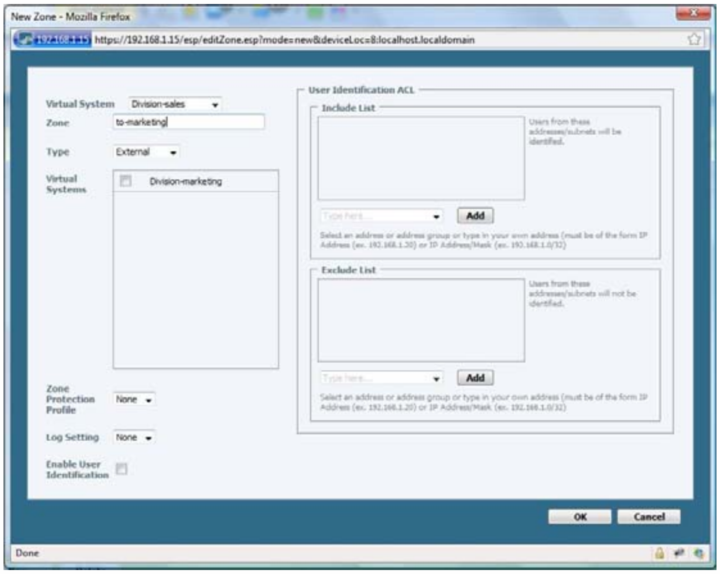
The first step is to create the two virtual systems. Note that the ingress and egress interfaces must either be part of the same virtual router, or part of two virtual routers that contain inter-VR static routes. Vsys2 is created with the name 'Division-sales' and vsys3 with the name 'Division-marketing'.



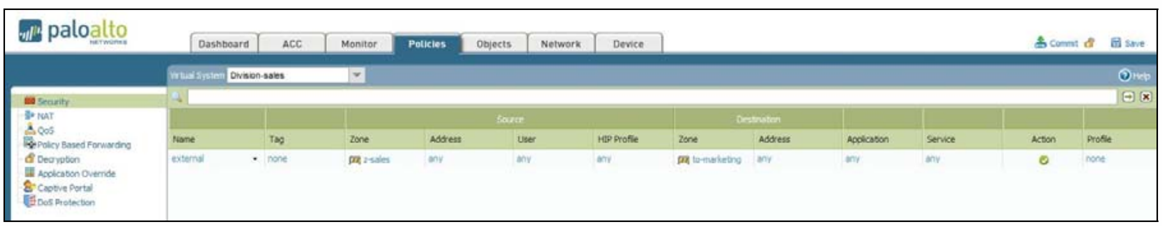
Next step is to make the virtual systems visible to each other. Make each virtual system visible to its counterpart using the last column In the example below we will make vsys3 visible to vsys2. Repeat this process to make vsys2 visible to vsys3.



The next step is to create the required security zone to allow the definition of the inter-vsys security policies. Creating a zone is done from the 'Network' tab in the GUI. Select 'New zone' from the zone-menu and create a zone of the type 'External vsys'. In the drop-down list select the vsys where the zone will be created for (virtual system) and select the virtual systems where the zone will allow traffic (if a policy exists) to that vsys or multiple vsys. Note that two security policies are required to allow inter-vsys communication (one permitting outgoing traffic which will have an external zone as the destination and another permitting incoming traffic which will have an external zone as the source).

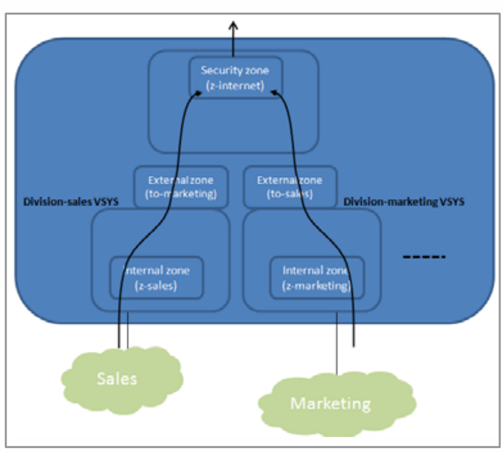


The final step is to create the required security policies. In the example below a security rule is created in vsys ‘Division-sales’ to allow traffic from security zone ‘z-sales’ to the external vsys security zone ‘to-marketing’. Note that a second security policy (not illustrated here) is required in vsys ‘Division-marketing’ from security zone ‘to-sales’ to ‘z-marketing’.



DEFINING A SHARED GATEWAY

A shared gateway lets multiple virtual systems share a single interface (typically connected to a common upstream network such as an internet service provider). Communications originating in a virtual system and exiting the firewall through a shared gateway require similar policy to communications passing between two virtual systems. An ‘External vsys’ zone is used to define security rules in the virtual system. Note that a shared gateway does not contain any security policies and therefore doesn’t require an ‘External vsys’ zone.



The Shared Gateway is configured from the ‘Device’ tab in the GUI.

ABOUT PALO ALTO NETWORKS

Palo Alto Networks next-generation firewalls provide customers with the ability to protect their network by identifying and controlling applications, users and content. There are three unique, enabling technologies within the Palo Alto Networks’ next-generation firewall: App-ID, User-ID, and Content-ID.

- **App-ID™**: The first firewall traffic classification engine to use as many as four different mechanisms to accurately identify exactly which applications are running on the network, irrespective of port, protocol, SSL encryption, or evasive tactic employed. The determination of the application identity is the first task performed by the firewall and that information is then used as the basis for all firewall policy decisions.
- **User-ID™:** Seamlessly integrates Palo Alto Networks firewalls with a range of enterprise directory (Microsoft Active Directory, eDirectory, Open LDAP) and terminal services offerings (Citrix, Microsoft Terminal Services), enabling administrators to tie application activity and security policies to users and groups – not just IP addresses. Captive portal and an XML API enable organizations to extend policies to those users that typically reside outside of the domain. User information is pervasive across all features including application and threat visibility, policy creation, forensic investigation, and reporting.
- **Content-ID™:** A stream-based scanning engine uses a uniform signature format to block a wide range of threats and limit the transfer of unauthorized files and sensitive data, while a comprehensive URL database controls web surfing. The breadth of threat prevention, done in a single pass, is unique to Palo Alto Networks and when combined with the application visibility and control delivered by App-ID, IT departments regain control over applications and related threats.

A complete set of traditional firewall, management, and networking features allows customers to deploy a Palo Alto Networks next-generation firewall into any networking environment.