TechNote:
Universal Security Gateway Architecture (MIPs, VIPs, and DIPs)

Introduction:
With the introduction of ScreenOS 3.1, NetScreen has enabled the use of multiple interfaces (beyond three) using a new ScreenOS architecture called the Universal Security Gateway Architecture (USGA). This architecture, however, goes well beyond simply supporting multiple interfaces, it provides a foundation for many new features and requires a slightly new way of configuring standard features. This application note will cover three key building blocks: Mapped IPs (MIPs), Virtual IPs (VIPs), and Dynamic IPs (DIPs) and will discuss changes to these building blocks with the introduction of ScreenOS 3.1.

This information is not designed to replace the Concepts & Examples guide, but rather to provide a comparison between the applications of similar features.

Definitions
Security Zone: Security Zones are logical points on the device where policy enforcement takes place. Security Zones can be the well-known security zones such as Trust, Untrust, and DMZ, or they can be user-defined Security Zones such as "Wireless_LAN" or "Finance_Department". Security Zones are dependent on interfaces (Physical or Virtual using VLANs) to actually pass the traffic, and also require Virtual Routers to determine the destination.

MIP: Mapped IP. This is not a new feature in ScreenOS. Mapped IPs are one-to-one mappings of IP addresses from the inside of the network to the outside of the network. The most common application of Mapped IPs is to map a private IP address on a server to a public IP address that can be routed and advertised to the public.

VIP: Virtual IP. This is not a new feature in ScreenOS. Virtual IPs are many-to-one mappings of IP addresses that distinguish traffic based on port number to determine what IP address to send the traffic to. The common application of VIPs is to have one public IP address represent the Web server, e-mail server, and FTP server, each of which has a unique private IP address. This sharing of one external IP address provides a good way to conserve expensive public IP addresses.

DIP: Dynamic IP. This is not a new feature in ScreenOS. Dynamic IPs help enable policy-based NAT as well as NAT before VPN encapsulation where overlapping private IP addresses exist in a VPN network.

Applications of MIPs, VIPs, and DIPs
Applications of the above three features are numerous and difficult to sum up. However, each serves a primary purpose.

1) MIPs, providing one-to-one address mapping: the scenario is simple. There are many servers on one DMZ, each of which has a private IP address. The company also

has a set of public IP addresses that is provided by their service provider. With Mapped IPs (MIPs), they can map the private IP addresses to the public IP addresses in a one-for-one mapping.

2) VIPs, providing one-to-many address mapping: primarily an application for small and medium-sized businesses where public IP addresses are expensive and hard to acquire. Using VIPs, multiple servers can share one public IP address by mapping port numbers to internal servers. For example, all incoming traffic on port 80 will be routed to the HTTP server, while all incoming SNMP traffic will be sent to the e-mail server.

3) **DIPs, providing policy-based address mapping:** DIPs are the multi-purposed tool for address translation. Applications include the following:
   - Many-to-many address translations. This can be used in VPN networks where connected sites have overlapping IP subnets. To allow them to be connected without IP address conflicts, IP addresses need to be translated either before the traffic is sent into the VPN tunnel or after it is decrypted at the other gateway. DIPs are used in either case to translated one subnet to another to allow overlapping networks to communicate with each other.
   - One-to-many address translations. This is often used when policy-based NAT is utilized. Policy-based NAT only translates traffic that meets the policy, allowing other traffic to be routed through the firewall. This allows for mixed networks of public and private IP addresses. This DIP application is very similar to NAT, except that it is done on a policy basis instead of by interface.

Changes to the functions in ScreenOS 3.1 (USGA and later)
ScreenOS 3.1 and the Universal Security Gateway Architecture has changed a few configuration features associated with the above three key features.
   - When a Virtual IP or Mapped IP is created, an address book entry will automatically be created in the Global security zone. This allows the VIP or MIP to be used by any policy for allowing or denying access to the VIP or MIP for from the VIP or MIP.
   - Virtual IPs are only supported on interfaces in the Untrust security zone as this is how VIPs are designed into the product. This is not a change from the previous ScreenOS architecture, but is noted as one of the few features not supported universally on all interfaces.
   - Dynamic IPs do not change with the new architecture.