A Guide to Secure VLANs for the NetScreen-1000 and the NetScreen-500 with Virtual Systems

May 2001

A White Paper by
NetScreen Technologies Inc.

Contents:

Introduction:

NetScreen Technologies offers two kinds of security devices - Appliances and Systems. NetScreen's line of integrated security solutions combines stateful-inspection firewall, IPSec virtual private networking (VPN), and traffic management functions. NetScreen's purpose-built devices feature near-wire-speed performance, even for 3DES encryption, and very low latency, allowing them to seamlessly fit into any network. NetScreen's security solutions are resilient devices that can scale to meet the needs of the most demanding large enterprise and service provider environments.

Enterprises use NetScreen security solutions to secure enterprise intranets, e-business operations and high-speed Internet access. Service Providers, such as Internet data centers (IDCs), application infrastructure providers (AIPs) and metropolitan area network (MAN) providers also use NetScreen solutions to protect their infrastructures. By using NetScreen's high-performance security systems, both enterprises and service providers can deploy modular systems that have the unique ability called Virtual Systems, a multi-customer architecture used in conjunction with VLAN technology that allows customers to create multiple security domains, either to secure discrete departments within an enterprise or as the basis for a service provider's managed security service.

This document will focus on NetScreen's line of Systems, specifically the NetScreen-1000 and NetScreen-500, which have this unique ability to implement the multisecurity-domain architecture called Virtual Systems.

Virtual Systems Overview

The NetScreen-1000 and NetScreen-500 allow for the creation of up to 100 Virtual Systems on the NetScreen-1000 and 25 on the NetScreen-500, each a unique security domain with its own address book, policies and management. This prevents one security domain's policies from interfering with the policies of another. IEEE 802.1Q VLAN tags are used to map Virtual Systems to security domains. NetScreen products using Virtual Systems and a corresponding VLAN switch, function as a combined security system with up to 100 ports, again each port with its own firewall and VPN policy, address book and management.

In enterprise environments, for example, this allows a NetScreen device with Virtual Systems to protect five corporate DMZs, three partner DMZs, two contractor DMZs, 10 internal departments, and have space for growth and scalability. In fact, NetScreen devices with Virtual Systems allow customers to define and protect any combination of internal/external DMZs, wired/wireless segments, trusted/untrusted domains, providing them with a scalability path to

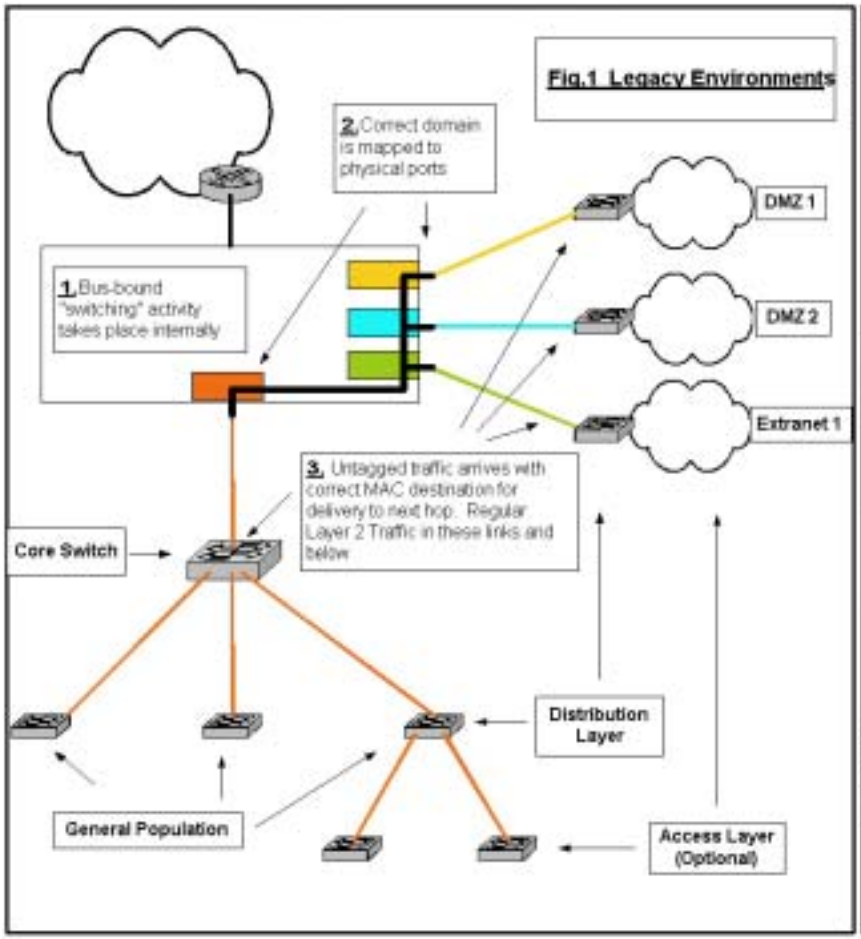
tackle the most complex environments. Running out of firewall DMZ ports is eliminated.

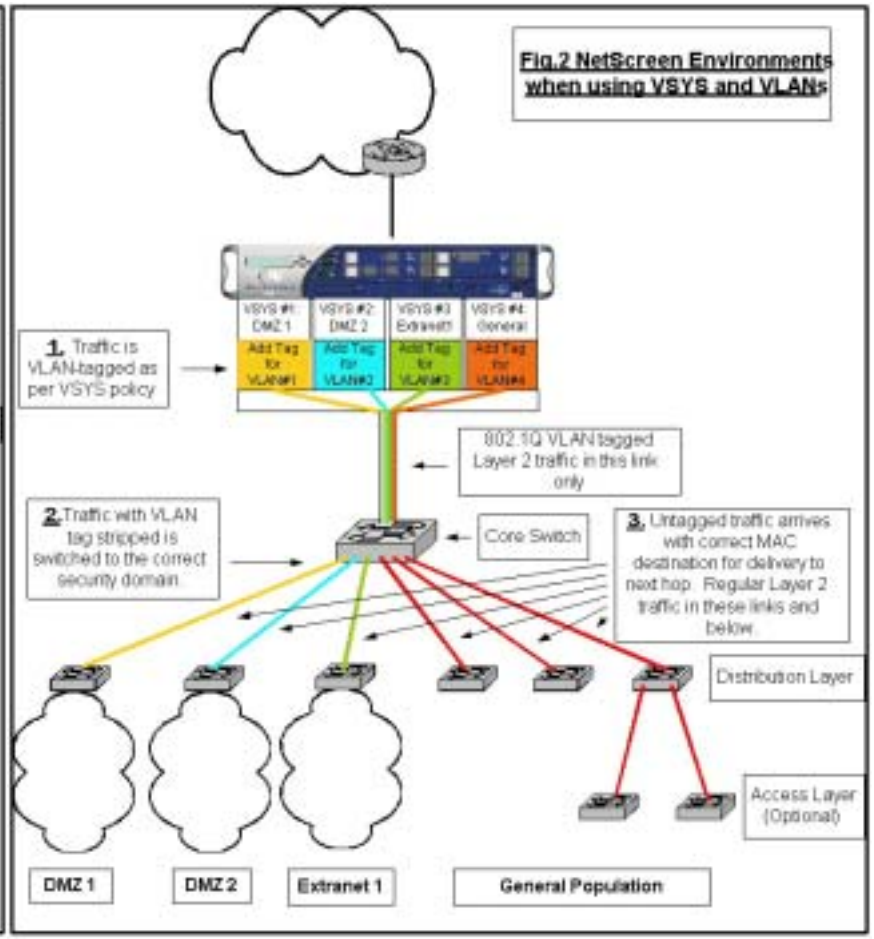
In service provider environments, such as an IDC, NetScreen's Virtual Systems and performance capabilities can support either a large single customer, the data center itself, or large numbers of customers requiring protection and secure connections.

In the case of NetScreen systems utilizing Virtual Systems, VLANs are used to map the separate resources within that security domain to its corresponding Virtual System. To illustrate the similarities and differences between the traditional, physical port-based approach and NetScreen's Virtual System approach, refer to Fig. 1 and Fig. 2. NetScreen's approach effectively allows a single high performance interface to replace the many expensive low speed interfaces traditionally used to add additional security domains to existing firewalls. NetScreen's internal architecture also eliminates the performance bottlenecks created in traditional software based firewalls with their PC architectures and multiple network interface cards. The traditional approach – based on physical ports - does not offer any security over NetScreen's approach using Virtual Systems.

There are five specific steps required to take advantage of NetScreen high performance firewall and VPN solutions, Virtual Systems, high-speed corporate infrastructures and an existing corporate security policy. In typical migrations from a traditional approach, only the core switch – and maybe a few distribution switches - would need any configuration changes, assuming it supports 802.1Q VLANs, which today is the norm. The rest of the infrastructure can remain untouched as per the existing corporate security policy.

Besides those steps, this document will conclude with guidelines for improving overall security, relevant for all switches and network devices, whether they participate in the security infrastructure or not.





Key Concepts:

A switch is essentially a self-learning Layer 2 bridge that forwards frames to the correct port for that node - this is done in hardware and carries a minimal latency cost. The other ports and segments do not receive those frames. This approach enhances the security of bridges and hubs by providing multiple collision and broadcast domains separated from each other, reducing repeated traffic and virtually eliminating the opportunities for network sniffing.

VLANs and 802.1Q tags are a powerful extension to layer 2 switches. One can define a logical group of systems that belong to the same logical segment (or Virtual Local Area Network [VLAN]) and use the switches to enforce the logical segregation between any two different VLANs - using special Layer 2 tags compliant to the 802.1Q specification.

The key aspect of switches – which contributes to both speed and security – is that lookup and processing of both the Layer 2 headers as well as the 802.1Q tag are performed in hardware. There is almost no opportunity for error in the processing of frames.

Virtual LANs as a multiplexing technique:

VLAN is a Layer 2 multiplexing technique that allows several streams of data to share the same physical medium while enjoying total segregation.

In the case of Virtual Systems, a special tag (802.1Q tag) is inserted by the NetScreen firewall on every Layer 2 packet. The downstream switch will read this tag and provide collision domain segregation and perform security domain partitioning. In a properly configured environment, this solution provides as much security as any multiplexing technique.

VLAN-type multiplexing techniques have been used in very secure environments for decades - for example Frame Relay or ATM - under very stringent security requirements and scrutiny.

Self-learning

Switches have sophisticated self-learning capabilities that allow them to be deployed with literally no configuration required. When a frame arrives destined to a specific MAC address, the switch will look into its MAC address table – the table mapping MAC addresses to port numbers. If the MAC is found, the frame is forwarded to the correct port. If the MAC is not found, the switch will broadcast the ARP request to all ports, will “learn” which port the answer comes from, and add that port entry in its MAC address table.

Layer 2 Frame:

The 802.1Q VLAN uses 12 additional bits in the Ethernet header in order to hold the tag. This required a change in the 802.3 Ethernet frame format. The 802.3ac standard defined the new Ethernet frame format that implements the 802.1Q VLAN information field. This standard was ratified in 1998. Nearly all backbone switches shipped in the last three years support this standard.

A “normal” (i.e. non 802.1Q) Layer 2 frame has the following format:

An 802.1Q Layer 2 frame has the following format:

A special 12-bit tag is added to provide segregation for as many as 4,096 security domains.

Tagging mechanisms:

There are mainly two ways to tag traffic - Implicit Tagging and Explicit Tagging.

Implicit Tagging will assign a tag to untagged frames based typically on which port it came from. This allows traffic coming from devices not supporting VLAN tagging to be implicitly mapped into VLANs.

Explicit Tagging requires that each frame be tagged with which VLAN it belongs to. This allows traffic coming from VLAN-aware devices to explicitly signal VLAN membership.

Secure Setup and Configuration – Core Switch and VLANs

Basic Steps:

As specified earlier, the following steps are to be performed on the Core Switch, as well as the Distribution Switches identified in the corporate security policy as requiring a high security posture (for example typically the switches in the DMZs.) Appendix A provides more details on basic topologies for medium security as well as high security posture.

When designing an infrastructure from scratch, users should refer to existing security architecture guides for correct deployment of the rest of the infrastructure. This will be out of scope for this document although general guidelines will be provided.

When existing VLANs need to span more than one switch, the same five steps need to be performed on every switch participating in VLANs.

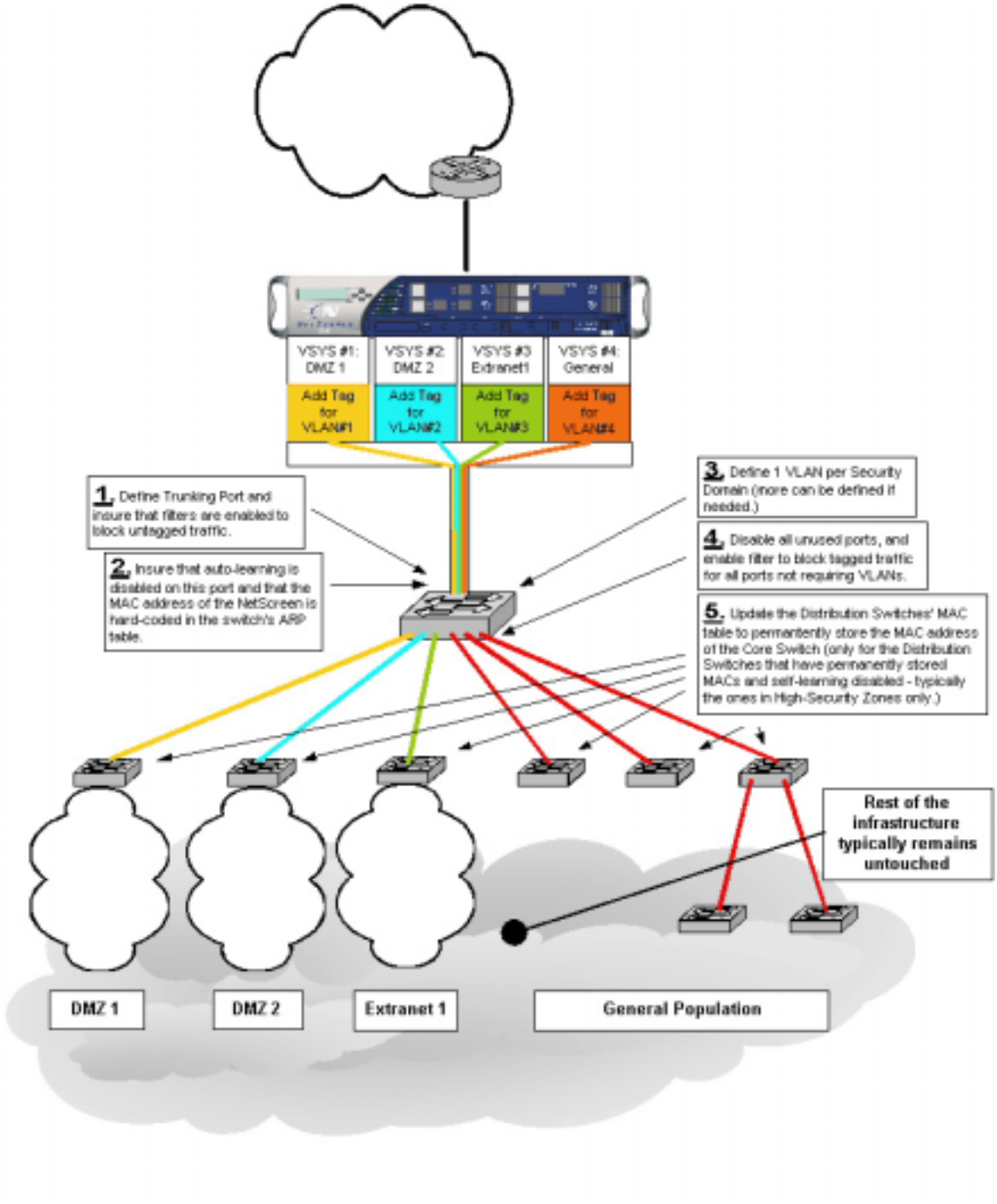
The five main steps to secure NetScreen Virtual Systems (VSYS) have been described in Figure 3. These are:

1. Define a unique trunking port for communication with the NetScreen device. Ensure that filters are enabled to block untagged traffic.
2. Ensure that auto-learning is disabled on that port and that the MAC address of the NetScreen is hard-coded in the switch's ARP table.
3. Define one VLAN per security domain (several VLANs can be assigned to the same security domain if needed).
4. Disable all unused ports, and enable filter to block tagged traffic for all ports not requiring VLANs.
5. For the Distribution Switches that permanently store MAC addresses and have self-learning disabled (usually only the Distribution Switches in High-Security Zones), update their MAC tables to permanently store the MAC address of the Core Switch.

Performing these basic steps and respecting the guidelines in the following section will provide optimal security posture. The traditional approach lacks any security advantages to this approach.

Figure 3. The Five Main Steps to Secure NetScreen VSYS/VLANs

This figure depicts the five main steps to secure NetScreen VSYS/VLANs. Distribution switches, access and workgroup switches are typically tightened only in high-security zones. The rest of the infrastructure remains untouched as per the corporate security policy.



General Guidelines:

The following are general guidelines that should be followed for all switches (Core, Distribution, as well as Access and Workgroup switches) with or without VLANs.

Physical Access

The Core Switch should be in a locked room where physical access can be controlled and monitored.

Update Policy

Users should always have the latest firmware and security patches for their switch, monitor the switch vendor's announcements for security bulletins, warnings and other patch releases. Ensure a process that can be used continuously and consistently.

Default Passwords

Change the default password for the default accounts created. Better yet, rename the default accounts and disable the default UserIDs, and change the default passwords to strong passwords (i.e. not easily guessed, and hard to brute force crack). Strong passwords incorporate at least three of following: lower case letters, upper case letters, numbers or non-alphanumeric characters and will be at least eight characters in length.

Unused Services

Disable all routing and all Layer 3+ services.

Unused Ports

Disable any unused port.

Auto Trunk Ports

In the case where disabling unused ports is not possible, it is important to ensure that ports that do not require trunking access should be set to "trunk off" or "no trunk," and filters should be enabled. This will guarantee that the switch will deterministically know what type of traffic to expect from which port and will discard any out-of-type frames.

MAC Hard-coding

Most switches allow for MAC addresses of hosts to be mapped to a specific port by hard-coding MACs. Thi, in effect, disables the self-learning features of the switch for that specific port and insures the correct mapping of MAC addresses to port number. Use MAC address hard-coding whenever possible.

VLANs and Trunk Ports

As mentioned in the previous section, enable filtering of untagged traffic on trunk ports and tagged traffic on non-trunk ports. This will ensure that the switch will deterministically know what type of traffic to expect from which port and will discard any out-of-type frames and will avoid unpredictable switch and/or end system behavior.

VLAN for Remote Management

Management VLANs should be turned off unless remote management functionality is absolutely necessary. In that case, it is important to define a separate VLAN for management purposes only (isolated from the rest of the topology) and access to the switch for management purposes should be authenticated and encrypted (using SSH/TACACS, for example).

Subnet Access with VLANs

Make sure that the switch is configured so that subnet-to-subnet connections are forced to go through a firewall so that appropriate security policies can be enforced.

Appendix A: Basic Topologies

This section introduces two basic environments – medium security environments and high security environments. For each environment, typical topologies are presented for both legacy Firewalls as well as NetScreen systems using Virtual Systems.

During a migration effort from legacy firewalls, typically only the core switch as well as the distribution switches in the high-security zone need to implement the five steps outlined in this document. The rest of the infrastructure can remain untouched as per policy.

Medium Security Environments

In medium security environments, only parts of the infrastructure enjoy a high security posture. Typically, the DMZs and critical domains are tightly managed, whereas the general population is governed under an easier to manage, less stringent security policy.

The following two diagrams (Fig.4 and Fig.5) depict environment comprising two security zones.

High Security Environment

In high security environments, the whole infrastructure enjoys a high security posture.

The subsequent two diagrams (Fig.6 and Fig.7) describe an environment comprising a unique high security zone.