



SECURITY WHITE PAPER

A vertical decorative graphic on the left side of the page, featuring a teal background with a white, curved, textured pattern that resembles a stylized leaf or a network path.

Create a Protected DHCP Network with Rogue Network Device Protection and Detection Utilizing The 3Com Embedded Firewall Solution

Creating a Protected DHCP Network with Rogue Network Device Protection and Detection Utilizing The 3Com Embedded Firewall Solution

By Neal Trieber, CISSP, MCSE, Principal Security Consultant
3Com Corporation

Exponential growth in distributed network connectivity fuels unauthorized rogue device access

Business Issue

Today's networks are inherently less secure than ever before with the necessary rise in practices like Business-to-Business (B2B) networking and outsourced contracted environments. In addition, the growth and need for telecommuting and Virtual Private Networking (VPNs) for distance networking and sharing of information has further blurred the lines between guarded perimeter and internal network access.

The exponential growth in shared systems has fueled the virulent onslaught of worms and threats brought on by the overwhelming growth in vulnerability and maintenance of today's networks. Remote and mobile users must now have greater access to the network leaving open opportunities for malicious and unauthorized access in addition to the damage caused by these acts.

Customers want direct access to their accounts and sensitive information to enable complete transactions online. Likewise, strategic partners require access to shared resources for efficient growth and conducting business. The challenge remains in giving trusted users the access they need to ensure continuity of business while keeping hackers and malicious threats from damaging the network and its resources.

The continued growth and widespread adoption of innovative broadband and high-speed enabling technologies coupled with the mainstream acceptance and availability of low-cost networking technologies has given rise to unauthorized or unknown devices attaching to corporate networks. As mainstream broadband components "find their way" into the corporate environment, they often times render the corporate network vulnerable allowing un-tethered and un-controlled access into the corporate domain.

In order to better combat the growing threat of unauthorized connectivity into the corporate infrastructure, deployment of a 3Com Embedded Firewall Protected Environment can give organizations the solution-set they need to both combat and mitigate the pervasive growth of un-controlled network access. The Embedded Firewall technology can simply deny access to any unauthorized devices. This capability only partially mitigates the risk. In order to optimally combat the issue, the Embedded Firewall Protected Environment can also help organizations immediately track-down, audit, log, and detain the unauthorized connection(s).

‘VLANs’ by themselves do not protect networks from ‘sniffing’ or ‘spoofing’.

Stop Your network from becoming a launch-point for attacks.

VLANs And Switched-Network Infrastructures Do Not Protect Networks From ‘Sniffing’ and ‘Spoofing’

The 3Com Embedded Firewall shifts the current paradigm in security by bringing network access control to the host-level in a hardware tamper-resistant format giving organizations the ability to disable host-level vulnerabilities like ‘spoofing’ and ‘sniffing’.

Many people have been falsely led to believe that by using Virtual Local Area Networks (VLANs), the data going through the switch can not be sniffed without special administrator configuration. Many people have been also led to believe that VLANs secure their network. VLANs by definition are not built for security or to secure a network. VLANs perform network segregation and separation by using special labeling called ‘VLAN tags’ and use a data encapsulation method called ‘VLAN frames’. ‘VLAN frames’ and their headers can also be spoofed in an attack known as ‘VLAN Hopping’.

Most networks that have VLANs deployed allow packets to route anywhere on the network including between different VLANs which does not help from a security stand-point.

In order to communicate on a network each host’s network port device must have its own unique Machine Access Control address (MAC Address) and a unique Internet Protocol (IP) address for communicating on a TCP/IP network.

‘Spoofing’ is the capability to misrepresent or fake the source

IP or MAC address of a packet of data. Spoofing itself is not an attack, but a technique used to hide or fake where data or an attack originates. By masking the source of an attack, spoofing can be used to shield an attack from being terminated by an alert administrator and make tracing the point-of-origin for the attack much harder to pin-point as the forged packets appear to come from fake hosts. A port-scanning tool such as the open-source tool ‘Nmap’ can be used to identify active ports or vulnerable applications. This same tool can generate data packets with random IP addresses or MAC addresses, masking the true source of the transmissions.

Large-scale retailers, web-merchants, and enterprise organizations have succumb to billions in lost revenue and downtime due to even small-scale Distributed / Denial of Service (D/DoS) attacks where the attacking hosts were able to elude authorities by ‘spoofing’ their originating addresses lengthening the time and fiscal compounding damage of the attacks. The organizations with compromised hosts that had been ‘hacked’ and used in the attacks were held liable in court for the damages incurred to by the victims.

The 3Com Embedded Firewall has next-generation anti-spoofing technology which enables it to protect itself from tampering by locking its IP and MAC addresses to its policy. This additional policy feature gives the 3Com Embedded Firewall the ability to stop any malicious program or user from abusing the host’s network communications to hide its originating address(es).

Employing switched networks by themselves do not protect networks from 'sniffing'.

The 3Com Embedded Firewall forces all packets to communicate properly with the host's proper source IP and MAC addresses. In addition the 3Com Embedded Firewall will also track all IP and MAC addresses for all incoming and out-going packets by performing reverse tracking to ensure that all data received comes from the actual source(s) that sent it in combination with its auditing and logging facility.

'Sniffing' data by itself is not an attack and is often synonymous with the act of capturing or spying on data packets as they traverse the network. 'Sniffing' is most often used to intercept data packets while they are in transit, which can then be read from the network to help troubleshoot communication issues. However, if the data is not encrypted or hidden in some manor, any data that is not protected or hidden can be read through any number of 'sniffer' or packet reassembly tools.

The 3Com Embedded Firewall features 3DES (pronounced 'Triple-Dez', or three times the U.S. Federal Government Digital Encryption Standard (DES) (168-bit)) IPSec (IP Security) VPN cryptographic acceleration hardware from its legacy 3Com 3CR990 architecture based on the 3XP™ RISC Processor.

The 3Com Embedded Firewall can take any data encrypted (hidden) with the Microsoft™ IPSec VPN client built-in to Microsoft™ Windows 2000, XP, and 2003 operating systems and accelerate the CPU host-intensive mathematics associated with calculating and maintaining the secrecy and security policies that use DES, 3DES, or the MD5 or SHA-1 digital signature technologies and have its IPSec

policies centrally managed through Microsoft™ Windows Active Directory™ or locally via the host system. IPSec used with 3DES encryption is considered one of the best technologies to encrypt data against sniffing and spying attacks to ensure privacy and is utilized in most Virtual Private Networks. (VPNs).

Another common misnomer sold to organizations is that by simply employing a switched-traffic network, data packets traveling through any particular switch or across its backplane can not be sniffed.

Some 'sniffer'-tools, like the open-source based 'ettercap', can fool a switch into thinking that its host is the network's router, and sniff right-through VLANs and switches. If data is not encrypted or hidden before it is sent from its source, an attacker can use a sniffing tool to obtain the root password for a server system or entire network infrastructure when an administrator initiates an administrative session either when the authentication information is sent to the server or device for authentication, or directly from the keyboard of the administrator's console if a 'sniffer' or 'sniffer'-based virus has been installed and infected the administrator's computer.

Once an attacker has a 'sniffer' installed on a network they can capture and steal any information, sensitive or otherwise, that is sent on the network because all data will pass in front of the 'sniffing' computer.



Once an attacker has obtained stolen administrative credentials (root-level access rights), not only can an attacker see your data, but they may also inherit the right to change it.

The 3Com Embedded Firewall solution can disable the mode that allows packet sniffing such that sniffing tools will yield no results except data that is actually intended and allowed by the 3Com Embedded Firewall network-wide security policy to be sent to that computer specifically.



**The 3Com
Embedded
Firewall stops
'sniffers' and
ensures
privacy.**

“DHCP is generally intended to make maintenance of remote and/or diskless hosts easier. While ..impossible, configuring such hosts with passwords or keys may be difficult and inconvenient. Therefore, DHCP in its current form is quite insecure.”

Vulnerabilities in Dynamic Host Configuration Protocol (DHCP) Serviced Networks

Today’s networks heavily utilize the Dynamic Host Configuration Protocol (DHCP) and its sibling TCP/IP protocol Dynamic Domain Name Service (DDNS) for dynamically automating the TCP/IP client addressing and administration of devices and hosts connecting to the network for access.

The Internet Engineering Task Force (IETF) Request For Comments (RFC) documents RFC 1541, RFC 1542, RFC 2131, and RFC 2132 respectively, govern the standards implementation of the Dynamic Host Configuration Protocol for IPv4 (DHCPv4) and DHCP options and BOOTP extensions for vendor implementations respectively.

“The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP) [7], adding the capability of automatic allocation of reusable network addresses and additional configuration options [19].”

As DHCP allows for automatic allocation of IP addresses and the majority of vendor implementations allows for ‘DHCP-By-Reservation’ (by which a host is assigned an IP address which has been specifically reserved for it using the host’s name or Machine Access Code/Control address (MAC), the actual RFC implementation specifications do not take any security

considerations into account. RFC 2131 states “DHCP is built directly on UDP and IP which are as yet inherently insecure. Furthermore, DHCP is generally intended to make maintenance of remote and/or diskless hosts easier. While perhaps not impossible, configuring such hosts with passwords or keys may be difficult and inconvenient. Therefore, DHCP in its current form is quite insecure.”

Though there have been many follow-on RFCs in regards to enhancing and updating the DHCPv4 standard, and whereas RFC 3118 respectively adds ‘DHCPAUTH’ for authentication of DHCP functions and messages, ‘DHCPAUTH’ is not a part of the majority of DHCP implementations. Thereby, DHCP remains a high-risk vulnerability in most networks with the ability to assign rogue or unauthorized devices automatic IP addresses with open communication access to the network.

The majority of current DHCP implementations do not take security or authentication at the device-level into account. Thus, DHCP has no mechanism for authenticating a device before it grants a device an IP address for access to the network. This vulnerability can allow hosts to connect to the network at-will and lease an IP address from a DHCP service on the network for use. Once the IP address has been assigned, the host receives full and open communication access to the network. This leaves the network vulnerable to hosts that can also statically ‘spoof’ or disguise itself as an acceptable or routable IP address and gain access to the network.

Rogue Device Protection and Detection

Typical DHCP-enabled networks become vulnerable to not having control over the ability to stop a host from 'sniffing' or 'spoofing' attacks because DHCP can not govern hardware-level access.

A DHCP-Server on a network is a host with an operating system like every other host on a network. The host-level connection represents the most vulnerable point of entry on any network from which the majority of threats enter or spread through an organization. Not having the ability to judge whether a device should be allowed to gain access to the network over and above authenticating the user of a host or device, leaves a high risk of vulnerability for allowing rogue or unauthorized devices access to network communications and private information.

The 3Com Embedded Firewall hardens the DHCP-Server by enforcing the missing layer of authentication security through its anti-spoofing technology to ensure and authenticate only the devices that have been approved and deployed by the organization with defined reservations can access the network and obtain an IP address for communicating. Furthermore, the 3Com Embedded Firewall solution adds the missing ingredient that protects the DHCP environment against rogue devices being able to 'spoof' themselves as approved devices on the network because the DHCP server is employing a 3Com Embedded Firewall with a 'No Spoofing' policy as well and only has reservations for approved devices. Any rogue device that

attempts to spoof an approved MAC address to obtain a reservation will be denied DHCP Server access by the 3Com Embedded Firewall.

Optionally, to optimally protect the network an additional address-pool in the DHCP-Server can be created called a 'Honey-pot' address pool.

In security, 'honeypots' are security resources used to lure attackers into thinking they have gained access or are using production systems or applications. In reality, the attacker has accessed a trap that has been set for them that audits and logs all of their activity to catch them in the act of their malicious behaviors or study their motives and techniques.

A 'Honey-pot DHCP address pool' would give a 'honeypot' IP address (I.e. an IP address in an unused or non-routable subnet like 10.X.X.X or 169.X.X.X) that is not in use on the network. The 'honeypot' IP address can be routable or non-routable on the network and can be used to audit and track the rogue's activities or simply set the 3Com Embedded Firewall Protected Network's policy to deny and audit any data sent from the 'Honey-pot DHCP address pool'.

Anyone who attaches a rogue or unauthorized device to the network will be audited, logged, and tracked. This gives organizations the true capabilities they need to not only stop rogue devices from attacking the network, but audit, catch, and even prosecute the individual or individuals by maintaining a chain-of-evidence and having the means to determine the location and control or detain the rogue device(s).

Create Rogue Device Protected DHCP Environment

Create a 'Honey-pot' trap for rogue or unauthorized devices.

Tangible Benefits with the 3Com Embedded Firewall Solution.

Enable a Secure Mobile-Protected Organization

Tangible Benefits With The 3Com Embedded Firewall Protected Network

Using the 3Com Embedded Firewall Policy Server, the organization can capture all of the MAC addresses of all of the hosts on their network. They can then export all of the MAC addresses of all of the hosts on their network and import them using scripting tools into their DHCP Server's database for employing DHCP-By-Reservation for each of the hosts on the network.

This will create a hardened double-layer of auditing and tracking for all devices approved and unapproved rogue devices that use or attempt to use the network.

Through deployment of a 3Com Embedded Firewall DHCP Protected Network, all of the hosts on the network including the DHCP-server will employ a 'No Sniffing', 'No-Spoofing', policy-enforced by the 3Com Embedded Firewall's 3XP Security Processor. The 3XP Processor provides hardware acceleration for all 3Com Embedded Firewall operations and policy management.

The 3Com Embedded Firewall protects its security policies and 3XP Processor by encrypting the policies and all communications from a 3Com Embedded Firewall to a 3Com Embedded Firewall Policy Server with 3DES encryption inside IPSec encapsulated tunnels. All 3DES IPSec communications from each 3Com Embedded Firewall are encapsulated inside TCP and UDP so the 3Com Embedded Firewall will still remain fully protected and retain full policy

enforcement operating behind other perimeter-level firewalls or NAT (Network Address Translating) routers or filters making them NAT and DHCP friendly. Each 3Com Embedded Firewall has its own unique keyed public-key-based relationship with its Policy Server. The Policy Server employs its own form of Public Key Infrastructure (PKI) to protect its policies and safeguard all communications with its Policy Servers. The Policy Server shares its public X.509 certificate with SHA-1 digital signature and RSA™ 1024 (1 megabyte) public-key with all of its subordinate 3Com Embedded Firewalls as well as assumes the role of Certificate Authority (CA) for the architecture.

The organization will again benefit by having created an environment that can not become readily used as a launch-point for attack against another host or network and held liable for such an attack against another party because it was without a 3Com Embedded Firewall DHCP Protected Network.

In addition the organization will also create a secure mobile-enabled workforce with protection that utilizes its own Location-Aware Intelligence™ to change its security policy to match the environment in which it resides so that the 3Com Embedded Firewall Policy will change to match the threat level of the environment in which it communicates.. The 3Com Embedded Firewalls are VPN-aware and can determine when they communicate with the corporate network through a VPN in addition to being IPSec accelerators.

The 3Com Embedded Firewall is Protection from the inside out.