Document #206156

Evaluating Wireless Intrusion Prevention Systems

Hands-on Examination of Products from Siemens, Cisco Systems and Network Chemistry Reveals Robust Capabilities of HiPath Wireless Manager HiGuard

A **white paper** commissioned by **Siemens**

THE TOLLY GROUP

WhitePaper

September 2006

THE TOLLY GROUP

TERMS OF USAGE

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors can occur.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. The Tolly Group provides a fee-based service to assist users in understanding the applicability of a given test scenario to their specific needs. Contact us for information. When foreign translations exist, the English document is considered authoritative. To assure accuracy, use documents downloaded from The Tolly Group's Web site.

This document was authored by:

Kevin Tolly,
President/CEO
The Tolly Group

Charles Bruno,
Executive Editor
The Tolly Group

TOLLY GROUP VENDOR SERVICE

With more than 17 years experience validating leading-edge Information Technology products and services; The Tolly Group has built a global reputation for producing accurate and unbiased evaluations and analysis. We employ time-proven test methodologies and fair-testing principles to benchmark products and services with the highest degree of accuracy.

Launched in 2003, The Tolly Group's "Tolly Verified" service provides in-depth, vendor-neutral certification of an array of features, functions and performance characteristics in technology disciplines as diverse as WLAN Switching and Anti-spam. See our "Tolly Verified" Home Page.

Our "Up-to-Spec" service provides the custom testing complement to the "standard", granular tests offered in "Tolly Verified". See our "Up-to-Spec" Home Page.

Plus, unlike narrowly focused testing labs, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure.

THE TOLLY GROUP

Table of Contents

THE TOLLY GROUP

Table of Contents continued

An effective WIPS must do three things well:

- Detect & automatically classify wireless devices & events — to figure out which are threats and which are not
- Prevent multiple wireless threats simultaneously while continuing to scan for new threats
- Accurately locate threats on a floor map — so they can be eliminated quickly

Products under test:

- Siemens HiPath® Wireless Manager HiGuard, SW ver. 2
- Cisco Systems' Cisco 4400 Series Wireless LAN Controller (SW ver. 4.0.155.5) and Cisco Wireless Control System (SW ver. 4.0.66.0)
- Network Chemistry RFprotect, SW ver. 5.0.7.2

Evaluating Wireless Intrusion Prevention Systems

Keeping Threats in Check

All enterprises face a new category of security threats created by wireless networking — whether or not they choose to install a wireless LAN. Every laptop computer today ships from the factory with built-in wireless capabilities. When these laptops are turned on, they automatically start looking for a wireless signal, and, if they find one, they'll start networking.

They may network with the authorized corporate network, or a neighbor's network across the street, or a honeypot AP deliberately placed by a hacker to steal their information, or even with another laptop computer if there's no WLAN in the area. In any of these scenarios, the enterprise network and security managers must protect the user's data, the laptop, and the network.

In addition, wireless APs are now so small and so inexpensive that rogue APs (APs unauthorized and unmanaged by the corporate IT department) are now a common phenomenon and a commonly understood threat. The majority of rogues are not attached to the network for malicious purposes, but they open holes in the network perimeter nonetheless. And then, there are rogues that are installed for illegal purposes, and it is vital that these be found and eliminated quickly.

In all of these cases, network managers must have the tools, and the processes, in place to deal with the litany of wireless threats.

Network managers utilize tools like 802.11i/WPA2 to encrypt traffic and authenticate users, but these only prevent a small fraction of the known WLAN security exploits. The primary tool being deployed in this security campaign across enterprises is the wireless intrusion prevention system (WIPS).

Unlike wired security devices, WIPS monitor the airwaves to detect wireless threats. A WIPS installation typically consists of a network server that communicates with wireless sensors or monitors that are distributed in the buildings/airspace that is being secured. Users need to understand that not all WIPS are equally effective at classification, prevention, and location of wireless threats.

Test Highlights — Siemens HiPath Wireless Manager HiGuard

- Detects 100% of the security threats launched against it, while Cisco and Network Chemistry products detected only about 38% and 72% of the attacks, respectively
- Prevents 100% of the threats automatically, while the Cisco 4400 WLC/WCS could only prevent 17% of them and required manual intervention on each threat, and Network Chemistry RFprotect prevented 55% of all attacks with some manual intervention
- Effectively prevents multiple threats simultaneously from a single sensor, while the competitive devices did not
- Continues to scan for new wireless threats even while preventing active threats
- Creates zero false alarms, unlike Cisco 4400 WLC/WCS which generated 14 false positives and Network Chemistry's RFprotect produced 11 — which amounts to a false-alarm range of 28% to 32%
- Locates wireless threats with a high degree of accuracy — within 4 meters in test scenarios, while Cisco and RFprotect devices were not as accurate

Moreover, while competitive WIPS solutions may indeed claim to offer many of the same security provisions, the degree and depth of those capabilities varies markedly. Given the mission-critical nature of the data and traffic traversing the corporate airwaves, it is imperative for network managers to understand the difference in protection afforded by various WIPS solutions.

For instance, while the vast majority of WIPS offerings suggest they can identify rogue APs and protect against them, the reality is that these products do so to very different degrees. While several systems may all identify a rogue AP, they may have vastly different success rates at so-called wireless blocking, where the WIPS instructs clients to cease communicating with the rogue AP(s).

Evaluating WIPS

Siemens commissioned The Tolly Group to evaluate HiPath® Wireless Manager HiGuard, a multi-faceted integrated WIPS designed to protect enterprise network infrastructures from wireless attacks. In addition to its WIPS functionality, HiGuard also provides RF management capabilities — such as heat maps showing RF coverage, reports on WLAN performance and usage, and simplified monitoring and troubleshooting of WLANs.

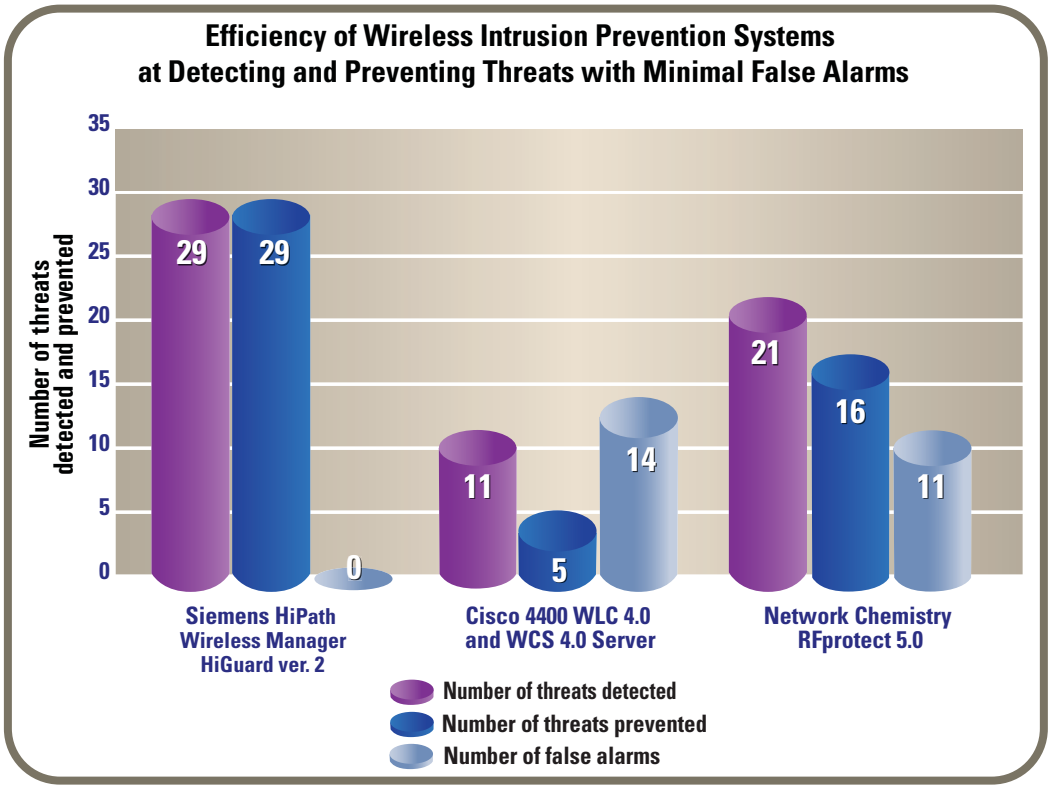
The Tolly Group assessed the capability of Siemens' HiGuard to detect and block a range of wireless threats — from dealing with rogue APs, to detection and prevention of access point (AP) MAC address spoofing, to detection and prevention of Denial of Service (DoS) attacks, and several others described below.

Tolly Group engineers measured the effectiveness of HiGuard against two other products: Cisco Systems, Inc.'s Cisco 4400 Series Wireless LAN Controller (WLC) and Cisco Wireless Control System (WCS), plus Network Chemistry RFprotect™ 5.0. Tests were conducted during August 2006.

Tests show that HiGuard detected all 29 of the threats launched against the networks and also blocked unauthorized traffic and prevented threats from inflicting network damage in 29 out of 29 scenarios. It did not generate any false alarms.

Competing devices were not nearly as effective, detecting only from 38% to 72% of the total threats, and preventing only about 17% to 52% of the threats — depending upon the product tested. (See Figure 1.) Moreover, the Cisco products generated 14 false alarms and the Network Chemistry product yielded 11 false alarms.

FIGURE 1



SOURCE: The Tolly Group, September 2006

Competitive Interaction

The Cisco and Network Chemistry products discussed in this white paper were acquired through normal product distribution channels. As both Cisco and Network Chemistry failed to respond and declined (respectively), test engineers configured devices according to vendor documentationThe Tolly Group invited officials from Cisco and Network Chemistry to participate in the testing, as specified by The Tolly Group's Fair Testing Charter. Both companies declined the invitation.

The Tolly Group invited officials from Cisco and Network Chemistry to participate in the testing, as specified by The Tolly Group's Fair Testing Charter. Both companies declined the invitation.

Rogue AP Detection and Prevention

In corporate LANs, rogue access points (APs) show up when employees or outside individuals deploy APs without the consent of the IT department.

Without the proper security configuration, rogue APs expose the company's network to the outside world. Ethernet jacks are ubiquitous, and it is a simple task to plug in an AP in order to provide wireless connectivity to anyone in the vicinity.

The Tolly Group verified the capability of the tested systems to detect rogue APs connected to the corporate wired network. To correctly identify APs as rogues, they must be both in violation of a company's security policy and connected to the corporate network on the local area network side. Violations can include incorrect SSIDs, lack of active encryption, etc.

Fourteen rogue APs, each with varying active services and features, were connected to the wired corporate Ethernet LAN. (See Figure 2, below.)

FIGURE 2

Rogue AP Configurations Used in Testing

Rogue AP	Product	Characteristics
Basic rogues		
RogueAP1	Belkin F5D7130	Bridge, no encryption, same VLAN
RogueAP2	Belkin F5D7130	Bridge, no encryption, different VLAN
RogueAP3	Belkin F5D7130	Bridge, WEP, same VLAN
RogueAP4	Belkin F5D7130	Bridge, WEP, different VLAN
RogueAP5	NETGEAR WGR614 v6	Router, sequential MAC, no encryption, same VLAN
RogueAP6	NETGEAR WGR614 v6	Router, sequential MAC, no encryption, different VLAN
RogueAP7	NETGEAR WGR614 v6	Router, sequential MAC, WEP, same VLAN
RogueAP8	NETGEAR WGR614 v6	Router, sequential MAC, WEP, different VLAN
Complex rogues		
RogueAP9	Airlink Ar325W	Router, cloned MAC, WEP, same VLAN
RogueAP10	Airlink Ar325W	Router, cloned MAC, WEP, different VLAN
RogueAP11	Linksys WRT54GS	Router, no DHCP, non-sequential MAC, no encryption, same VLAN
RogueAP12	Linksys WRT54GS	Router, no DHCP, non-sequential MAC, no encryption, different VLAN
RogueAP13	Linksys WRT51AB	Router, default configuration, WEP, same VLAN
RogueAP14	Linksys WRT51AB	Router, default configuration, WEP, different VLAN

SOURCE: The Tolly Group, September 2006

Pre-standard 802.11n APs tested:

- **Linksys WRT54GX Wireless G Broadband Router with SRX**
- **Belkin Corp. Wireless Pre-N Router F5D8230-4**
- **Buffalo Technology, AirStation™ Nfiniti Wireless Notebook Adapter (WZR G300N)**

Tests show that Siemens' HiGuard detected all 14 rogue APs in less than one minute, and was the only WIPS that was able to identify the subnet to which the rogue AP was attached.

By contrast, Cisco's WLC/WCS tandem detected just four of the 14 rogue APs as connected to the enterprise network, and took much longer, even in a simple dual switch network. The average detection time was about 20 minutes.

Network Chemistry's RFprotect automatically detected eight of the 14 rogues, but required the intervention of an engineer in six of those eight cases. In only two of our test cases rogue APs were identified correctly and automatically prevented. In the other 12 test cases, the RFprotect system log showed it was checking on the rogue APs, but it failed to identify them as rogues within our one-hour test window. After one hour, we manually prompted the RFprotect system to check each individual rogue AP, and then it was able to identify six additional threats, but it still failed to detect the remaining six as rogues.

A relatively new issue in the WLAN and WIPS arena — is the emergence of a number of "pre-standard 802.11n" APs which are designed to provide the user with more bandwidth or extended range. These APs create a new class of security threat — as they transmit traffic and associate with clients using a non-standard protocol and thus might be used by a hacker to steal data — undetected by a WIPS that is only monitoring the standard 802.11 a/b/g protocols.

Of the three systems tested, only the Siemens' HiGuard was able to correctly identify these pre-standard 802.11n APs and alert the administrator to their presence and potential threat. The other two systems tested were unable to distinguish them from standard 802.11 APs.

An Ounce of Prevention

Over-the-air blocking or prevention is required to deal with ad-hoc connections, client mis-association, and other wireless threats. Wired-side blocking or prevention cannot address these threats.

Detecting wireless threats, such as rogue APs, of course, is only half the battle. The other half is isolating these threats, e.g. rogue APs and stopping clients from communicating with them.

Generally speaking, when a WIPS detects a rogue AP, it should automatically invoke a protection facility to interact with client devices and instruct them to cease communications with the rogue AP. In effect, the WIPS attempts to interrupt the session state between the rogue AP and the clients. This prevention should apply to both authorized (internal, enterprise) clients as well as unauthorized (external) clients.

Rogue Prevention Notes:

Cisco could not prevent Centrino clients from associating with rogue APs during testing

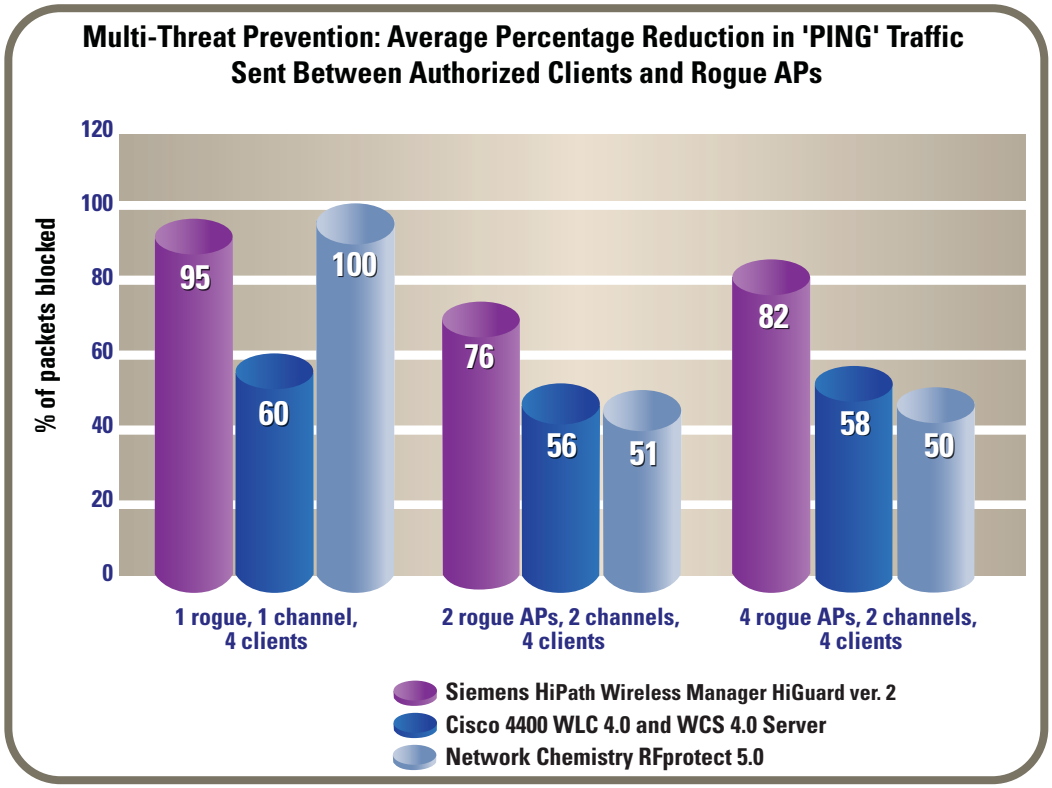
Network Chemistry only prevented traffic on one channel per sensor during testing

The Tolly Group verified the ability of HiGuard and the other products tested to prevent clients from accessing a corporate network via rogue APs.

Once a rogue is identified, a WIPS should be able to disconnect clients from the rogue AP. A WIPS also should be able to use a single sensor to detect and prevent multiple simultaneous security breaches by stopping multiple clients from accessing multiple rogue APs. A single sensor's limitations are often overlooked when blocking multiple threats, but important in real-life deployment scenarios. The Tolly Group also tested these scenarios.

Tests show that HiGuard successfully detected and automatically prevented all 14 individual rogue threats and three different scenarios involving multiple simultaneous threats on a single sensor, one HiGuard sensor was able to detect and block four rogue APs transmitting across two channels. (See Figures 3 and 4.) This demonstrates that HiGuard successfully was able to throttle back communications between the client devices and the rogue APs to the point where it was effectively stopped.

FIGURE 3



SOURCE: The Tolly Group, September 2006

One key security issue created by wireless is authorized (enterprise) clients connecting to external WLAN networks. Client mis-association, Honeypot APs, AP MAC spoofing, and ad-hoc networking are different forms of this threat.

By comparison, Cisco's WLC/WCS tandem required manual intervention to prevent the four out of the 14 rogue APs it could detect, while Network Chemistry's RFprotect automatically prevented eight of the individual 14 rogue threats, once they were (manually) detected.

However, in the multiple simultaneous rogue scenarios, both the Cisco and the Network Chemistry products demonstrated weaknesses. Cisco's WLC/WCS could not effectively prevent Centrino clients, showing only 30% effectiveness, while Network Chemistry's RFprotect only prevented traffic on one channel, being ineffective on the second channel.

Test results underscore that HiGuard's rogue AP prevention performance consistently outperformed Cisco's WLC/WCS and Network Chemistry RFprotect for all the scenarios tested. Tests also show that only HiGuard delivers the ability to detect consistently and prevent rogue AP sessions. The test criteria were set to require 65% blockage of any connection to be deemed "effective" prevention.

Client Mis-association

Because WLAN signals can travel through walls, it is possible for a corporate WLAN user to connect — or "associate" — deliberately or accidentally with an AP "outside" of the corporate network. (This can happen very easily if said AP is not protected by WEP or another method.) Corporate clients using these systems inadvertently can be exposing password and other company information to outside hackers as they communicate to Web resources over this "open" WLAN.

Legitimate clients should be authorized automatically when they connect to a corporate LAN through a wireless connection. They then should be prevented from associating with an unsecured non-corporate AP, either accidentally or deliberately. The Tolly Group examined the capability of each of the WIPS (the DUTs) to detect and prevent corporate clients from sending traffic through external APs.

In the test, engineers first verified so-called "client auto-classification," where a new client attempts to join the wireless network and establish communications with an AP. The WIPS must auto-classify the device as an authorized or unauthorized user and take the appropriate action(s).

FIGURE 4

Wireless Threat Detection and Classification

	Test scenarios	HiPath Wireless Manager HiGuard ver. 2	Cisco 4400 WLC 4.0 and WCS 4.0 Server	Network Chemistry RFprotect 5.0
	Available APs			
Classification	Wired Rogue AP Auto-classification	Yes	Yes	Yes
	External AP Auto-classification	Yes	No	Yes[1]
	WLAN Client Auto-classification	Yes	No	Yes[1]
	Pre and Draft 802.11n Auto-classification	Yes	No	No
	Rogue APs			
Threat detection	Single Rogue AP detection (14 Different APs)	14 out of 14	4 out of 14[2]	8 out of 14[3]
	Multiple threat detection (4 clients)—1 Rogue AP—1 Channel	Yes	Yes[2]	Yes
	Multiple threat detection (4 clients)—2 Rogue APs—2 Channels	Yes	Yes[2]	Yes
	Multiple threat detection (4 clients)—4 Rogue APs—2 Channels	Yes	Yes[2]	No
	Client Mis-association	3 out of 3	0 out of 3	3 out of 3
	Adhoc Networks	3 out of 3	2 out of 3	3 out of 3
	AP MAC Address Spoofing			
	Local AP MAC address spoofing	Yes	Yes	Yes
	Remote AP MAC address spoofing	Yes	No	Yes
	Honeypot Attack	Yes	No	No[4]
	Misconfigured AP			
	Security Misconfiguration	Yes	No	Yes
	Network Misconfiguration	Yes	No	No
	DoS Attack	Yes	Yes	Yes
	Total Threat Detection	**29 out of 29**	**11 out of 29**	**21 out of 29**

Notes:

1. **No default auto classification for APs or clients; may require significant expertise to configure**
2. **Detection for bridges only; average detection time was 20+ minutes**
3. **Only two threats were identified automatically within one hour; six other rogues were identified with manual prompting**
4. **An "Unauthorized AP is using authorized SSID" alert exists, but did not trigger**

SOURCE: The Tolly Group, September 2006

Auto-Classification

In the test scenario, engineers powered up CorporateAP1 and CorporateAP2, representing two authorized APs on the network. Next they powered up four unknown, uncategorized clients which attempted to join the wireless LAN and communicate with the APs. (These clients represented new employees or newly issued PCs.)

An 'unauthorized client' is a client that has not been authorized for activity on the corporate network. An unauthorized client may attempt to gain access to resources connected to the corporate LAN through the rogue AP. (In wireless jargon, this is called "associating" with the rogue AP.)

For the test, engineers used one Centrino-based 802.11 b/g client, one Cisco-based 802.11 a/b/g client and two Linksys 802.11 a/g clients.

Only Siemens' HiGuard was able to properly auto-classify all of the clients. The Cisco WLC/WCS relied on higher level authorization from the network. The Cisco system only keeps track of what devices are attached to the Cisco WLAN network, and reports everything else as external. This is a fundamental issue and a weakness with respect to tracking and catching an entire class of wireless threats. The Network Chemistry RFprotect product does have an auto-classification capability, but it is disabled in the standard configuration. Our test engineers (who have a significant level of WIPS expertise) found it extremely difficult to configure the auto-classification feature securely and resorted to manual authorization of the clients. (See Figures 4 & 5.)

FIGURE 5

Wireless Threat Prevention

Test scenarios	HiPath Wireless Manager HiGuard ver. 2	Cisco 4400 WLC 4.0 and WCS 4.0 Server	Network Chemistry RFprotect 5.0
Rogue APs			
Single Rogue AP prevention (14 Different APs)	14 out of 14	4 out of 14[1]	8 out of 14[2]
Multiple threat prevention (4 clients)—1 Rogue AP—1 Channel	Yes	No[1,3]	Yes
Multiple threat prevention (4 clients)—2 Rogue APs—2 Channels	Yes	No[1,3]	No[4]
Multiple threat prevention (4 clients)—4 Rogue APs—2 Channels	Yes	No[1,3]	No[4]
Client Mis-association	3 out of 3	0 out of 3	1 out of 3[3]
Adhoc Networks	3 out of 3	1 out of 3[1,3]	3 out of 3
AP MAC Address Spoofing			
Local AP MAC address spoofing	Yes	No	No
Remote AP MAC address spoofing	Yes	No	No
Honeypot Attack	Yes	No	Yes[5]
Misconfigured AP			
Security Misconfiguration	Yes	No	Yes
Network Misconfiguration	Yes	No	No
DoS Attack	Yes	No	No
Total Threat Prevention	**29 out of 29**	**5 out of 29[6]**	**15 out of 29**

Notes:

1. Not automatic; engineers were forced to use manual initiation

2. Detection had to be manually initiated in six of eight test cases

3. Device failed to prevent Centrino clients

4. Tested devices must prevent multiple threats on multiple channels; device failed to prevent threats on a second channel

5. As a client misassociation

6. Cisco would have scored 0 out of 29 if automatic prevention was a requirement

SOURCE: The Tolly Group, September 2006

Preventing Client Mis-association

In this portion of the test, engineers sought to determine the effectiveness of the WIPS at preventing clients from associating to a non-corporate AP, either accidentally or deliberately.

For the mis-association portion of the test, engineers powered up external APs representing a neighboring company's APs and then associated four authorized clients (a Centrino client, a Cisco a/b/g client, and two Linksys 802.11 a/g clients) with the unauthorized external APs. Engineers examined each of the WIPS to determine if they properly detected the mis-associations. On the prevention side, engineers examined the extent to which the WIPS enabled wireless blocking with the external APs and the resulting frame loss from PING traffic between the clients and the external APs or the neighboring APs.

Siemens' HiGuard detected and simultaneously prevented all four clients in all three test scenarios from transmitting traffic through any unauthorized external AP. This demonstrates that HiGuard can recognize multiple new clients attempting to gain access to the external AP. (See Figures 4 and 5.)

The Cisco 4400 WLC/WCS was unable to detect any of the instances of clients transmitting traffic to an unauthorized external AP as a security threat. The Cisco product lacks the concept of client mis-association — once a client disconnects from the Cisco WLAN, it becomes indistinguishable from a neighbor's client/PC.

Network Chemistry RFprotect was able to detect clients communicating with the external APs. However, as in the rogue AP prevention tests, Network Chemistry RFprotect concentrated its prevention ability onto one channel and neglected the second channel. It is a downside that RFprotect cannot prevent mis-associations across more than one channel without installing multiple sensors and driving up their costs.

Moreover, tests reveal that a client mis-association will usually result in the Cisco 4400 WLC/WCS creating a false rogue AP alarm. As an example, if a worker on the Cisco WLAN disconnects from the enterprise network and logs into a neighboring business' WLAN (or the hotspot at the coffee shop across the street) during a lunch break to peruse the Web and then logs back into the corporate WLAN when finished — this will result in the Cisco WLC/WCS reporting that neighboring AP as a rogue AP. We also observed this behavior in about 30% of the cases with Network Chemistry. This obviously would create challenges for any network administrator and would prevent them from using

Both the Cisco and Network Chemistry systems generated false rogue alarms — after a client mis-association had ended — identifying the external/neighboring AP as a rogue.

automatic rogue AP prevention in this environment. The Siemens' HiGuard did not exhibit this behavior.

Ad-hoc Networks

In wireless networks, sometimes clients attempt to form an ad-hoc network with other clients using their wireless capabilities, without going through any AP. Because of the dangers hackers can pose — exploiting unknowing users' ad-hoc connections, WIPS should be able to detect and block the formation of such ad-hoc networks, when they involve any authorized client.

For this test, engineers authorized one client laptop and did not authorize a second laptop. They created matching ad-hoc profiles in each laptop and established ad-hoc networks between the laptops with PING traffic flowing between them. Engineers first examined whether the DUTs identified and classified the ad-hoc traffic as a threat. Then, they tested to see if the WIPS could prevent the ad-hoc traffic by instructing the authorized client to throttle back communications with the unauthorized client. This is typically called wireless blocking. The WIPS blocks the traffic to an unauthorized client(s) by preventing authorized clients from communicating with the unauthorized devices.

Engineers verified the blocking by measuring the amount of frame loss to and from the unauthorized client.

Both the Siemens' HiGuard and Network Chemistry RFprotect successfully detected three out of three unauthorized client attempts to form ad-hoc networks with legitimate clients. (See Figures 4 & 5.) The HiGuard system blocked an average of 100% of the traffic from the three different ad-hoc networks; likewise, RFprotect blocked an average of 97% of traffic from legitimate clients to the ad hoc network clients, while in contrast the Cisco 4400 WLC/WCS failed to block any traffic for two of the ad-hoc networks.

The Cisco product had significant limitations dealing with this threat. As reported earlier, the testers could not find the concept in the Cisco product of authorized (enterprise) vs unauthorized (external) clients. Without this construct the Cisco WLC/WCS was unable to distinguish between an ad-hoc connection between two neighbor clients and an ad-hoc connection between a hacker and an enterprise laptop. As a result, engineers were unable to determine which ad-hoc connections represented a threat, and the product did not automatically prevent them.

When manually prompted, the Cisco product readily performed wireless blocking of an ad-hoc connection between two Cisco 802.1 a/b/g clients. However, it was unable to block an ad-hoc connection between two Intel-based Centrino clients.

The Cisco 4400 WLC/WCS

- **Could not distinguish between authorized (corporate) and unauthorized (external) clients/laptops when looking at ad-hoc connections**
- **Could not stop an ad-hoc connection between two Centrino clients**

This is particularly noteworthy since the vast majority of wireless devices shipped today support Centrino chipset technology. And, to the testers' surprise, the Cisco WLC/WCS failed to detect an ad-hoc connection between two Linksys clients.

As above, the ad-hoc test scenario revolved around a single sensor, as non-overlapping sensor coverage is commonplace. It is possible that under a test scenario with multiple sensors, the Cisco behavior might change.

AP MAC Spoofing

All WLAN AP equipment is shipped from the factory with MAC address(es) installed for the wireless interface.

Standard tools (downloadable from the Internet) can allow a hacker to "spoof" these MAC addresses to pose as an authorized AP thereby getting clients to associate to him - and enabling him to eavesdrop on their credentials and information. This is the first step in creating a "man-in-the-middle" attack or an "evil twin" attack.

Only Siemens' HiGuard was able to detect and prevent a remote AP MAC spoofing attack.

For this test scenario, an external AP copied the corporate AP's MAC address and SSID in order to appear identical. Clients will normally associate with the AP with the stronger signal. Clients may associate initially to the spoofing AP, or even transfer the connection during a transaction due to signal strength.

Engineers first examined the ability of the DUTs to detect and prevent local AP MAC spoofing - that is, when the un-authorized AP resides in the same physical vicinity as the AP it is spoofing — such that it can be "seen" by the same WIPS sensor.

For the Local MAC spoofing test, engineers used a Cisco LWAPP AP as the corporate AP and Dell Latitude D600 laptop with Linksys WPC55AG Wireless 802.11 b/g card running Linux KNOPPIX open source bootable CD with Operator software as the spoofing AP. Engineers configured the Operator software to perform MAC spoofing and placed these APs close enough to be visible to the same sensor. Engineers examined whether the WIPS under test identified that two devices used the same MAC address and prevented traffic from an authorized client to pass to the spoofing AP.

All three products successfully detected the unauthorized AP spoofing a local AP, but only the HiGuard successfully blocked the spoofing AP. Moreover, even though all three products detected the local spoofing AP, HiGuard did so in under one minute, while the Cisco and Network Chemistry products needed 8 to 10 minutes to find the spoofing AP. (See Figure 6.)

FIGURE 6

AP MAC Spoofing Detection and Prevention Comparison

	HiPath Wireless Manager HiGuard ver. 2	Cisco 4400 WLC 4.0 and WCS 4.0 Server	Network Chemistry RFprotect 5.0
Local LWAPP MAC Spoofing			
Detection (Time to detect)	Pass < 1 minute	Pass < 10 minutes	Pass < 8 minutes
Auto Prevention	Pass	Fail	Fail
Remote LWAPP MAC Spoofing			
Detection (Time to detect)	Pass < 1 minute	Fail	Pass < 10 minutes
Auto Prevention	Pass	Not supported	Fail
Approximate location	Pass (2 sensors indicated)	Not supported	Fail

Note: In Approximate Location tests, two sensors were used for each of the WIPS products under test.

SOURCE: The Tolly Group, September 2006

For the remote spoofing test, engineers introduced a second sensor and set up the test bed such that one sensor saw only the corporate AP and another saw only the spoofing AP.

When engineers tested remote spoofing — where an unauthorized AP spoofs the MAC address of an AP in another physical location (not visible to the same WIPS sensor), both Siemens' HiGuard and Network Chemistry's RFprotect detected the attack, but only Siemen's HiGuard prevented the security incursion.

In this test, Network Chemistry's RFprotect needed eight minutes to detect the remote spoofing AP — versus under one minute for HiGuard. The Cisco 4400 WLC/WCS failed to detect the remote spoofing device altogether.

Honeypot Attacks

One serious lower-layer attack that exploits client weaknesses is the honeypot AP. In the wireless realm, a "honeypot" is an attacker's AP that is set up in close proximity to an enterprise, falsely advertising the same SSID as the enterprise's legitimate AP. The goal of such an attack is to lure authorized clients to associate with the honeypot AP. From that point, a security attack can be mounted, or an attempt can be made to learn the client's authentication credentials. Most client

The Cisco WLC/WCS system does not have an alert for a Honeypot attack — the product does not attempt to detect this kind of event.

devices have no way of distinguishing between a valid AP and an invalid one — the devices only look for a particular SSID and will associate to the nearest AP advertising that SSID.

In a honeypot AP, the duplicate SSID can be a deliberate deception or the result of poor configuration, as when neighbor networks have been setup with default SSIDs from the same vendor.

Engineers configured CorporateAP2 (a Cisco LWAPP AP) as a legitimate AP and configured another AP as the "honeypot" by giving it an SSID matching CorporateAP2. Engineers then verified that the DUTs recognized that the honeypot AP utilized a different MAC address, and then consequently verified that the DUTs' prevention policies blocked traffic with the honeypot by witnessing the frame loss of PING traffic between clients and the honeypot AP — such frame loss amounts to wireless blocking, since clients are blocked from communicating with the honeypot AP.

All three systems saw the honeypot AP in the air, but only the Siemens' HiGuard correctly identified it as a threat. The test showed that only Siemens' HiGuard successfully detected and prevented the honeypot attack.

During the test, the Network Chemistry RFprotect did not alert the administrator that a honeypot attack was occurring, but still defended against it because it characterized the attack as a client misassociation. (See Figure 7.) [*Note: The Network Chemistry RFprotect system does have an alert for "AP using same SSID as authorized AP," but the alert was not triggered during the test.*]

The Cisco 4400 WLC/WCS failed to detect and prevent the attack. Interestingly, the Cisco product does not even have an alert or alarm for this kind of threat. The system does not appear to be designed to contain wireless traffic or prevent users from associating with external APs (malicious or not).

FIGURE 7

Honeypot Detection and Prevention Comparison			
	HiPath Wireless Manager HiGuard ver. 2	Cisco 4400 WLC 4.0 and WCS 4.0 Server	Network Chemistry RFprotect 5.0
Honeypot detection	Pass	Fail	Fail
Honeypot prevention	Pass	Fail	Pass

SOURCE: The Tolly Group, September 2006

Misconfigured APs

Only Siemens' HiGuard was found to enforce different WiFi security policies on different VLANs. This enables an enterprise to set different WLAN policies for various functions, different parts of a building, or even multiple sites.

There are several scenarios where corporate APs may be accidentally misconfigured or mislocated (attached to the wrong subnet). WIPS systems should enforce the company's security policy, alert the network administrator to such events, and prevent authorized clients from connecting to a corporate AP that has been misconfigured.

Testing determined that while it is not possible to misconfigure a single Cisco AP (because the configuration is downloaded from the WLC), it is possible to misconfigure a WLAN in the WLC and thus all the APs that are attached to it.

Tests showed that both HiGuard and RFprotect were able to prevent users from connecting to a corporate AP where encryption has been turned off in violation of a security policy. However, the Cisco WCS has no alert if one of its managed WLC switches has been reconfigured incorrectly, turning off encryption or otherwise changing the configuration on one or more of its WLANs. The administrator would have to discover this by a manual search or from a user report,

Next, engineers subjected the devices to a network misconfiguration where "Corporate AP1" was placed in VLAN2, which was a violation of the corporate security policy. (See Figures 4 and 5.) This might represent a scenario where an enterprise creates a special VLAN for guest access — and allows APs to be installed on this VLAN, but at the same time prohibits APs on the other VLANs in the building.

Tests show that only HiGuard was able to detect the network misconfiguration scenario and prevent clients from associating with an unauthorized AP. This scenario does not apply to the Cisco WLC/WCS combination — as each AP is assigned to a specific VLAN when the WLAN is configured.

Alarming Numbers

False or spurious DoS alarms after first eight hours of testing:

HiPath	0
Cisco	72
NC	57

- **Cisco WCS only aggregates 24 hours worth of alarms, making a three-day evaluation impossible**
- **Network Chemistry reports DoS alerts on unauthorized APs**
- **At the end of 48 hours, HiPath reported 22 DoS attacks, Network chemistry reported 667**

Denial-of-Service Attacks

Wireless Denial-of-Service (DoS) attacks attempt to broadly disrupt network wireless connections by sending broadcast "de-authenticate" commands over the air. A broadcast deauthentication will force clients to disconnect from the AP. As wireless Voice over IP becomes more widespread, the threat of this type of disruption becomes more critical.

Tests show that all three products tested successfully detected DoS attacks, but only Siemens' HiGuard blocked the DoS attacks with no degradation of throughput.

The Cisco 4400 WLC/WCS and the Network Chemistry RFprotect were able to detect the DoS attacks, but they were unable to protect against the attacks by responding with network blocking.

Note: The test was run with Cisco's Management Frame Protection both enabled and disabled, but this had no apparent effect on the results.

False Alarms

A key issue for any security system is false alarms. A security system that creates volumes of false or unnecessary alerts or alarms — will quickly be ignored or tuned out, if not turned off.

During our testing, engineers determined that they could create false alarms on the Cisco and Network Chemistry systems — on demand. There are certain patterns of behavior which are guaranteed to create false rogue alarms on these systems. In addition to the false rogue alarms, engineers also found that they could create false MAC spoofing alarms on the Network Chemistry system with regularity. And finally, during testing we also found both the Cisco and Network Chemistry systems generated a significant number of false DoS attack alarms. In one eight-hour stretch, the Cisco WLC/WCS produced 72 DoS alerts. The Network Chemistry RFprotect also generated 57 false DoS alarms during the same eight-hour period. However during the test period, the Siemens' HiGuard system did not generate a single false alarm.

Such inaccurate data is a burden for overtaxed network administrators who must wade through the morass to determine which events are real and should be acted upon. This in turn can result in administrators actually under-reacting to real security threats.

Location Tracking

It is of significant benefit for a WIPS to not just detect a rogue AP or other disturbance, but to pinpoint with accuracy the location of the device so network personnel can unplug it. Such a capability is called location tracking and almost every WIPS claims to offer it to some degree.

Engineers measured the accuracy of the location tracking feature of the DUTs in different test scenarios; varying the AP location and transmit power levels. Test results show that Siemens' HiGuard located the APs with a high degree of accuracy, but neither the Cisco 4400 WLC/WCS nor the Network Chemistry RFprotect located the APs with the same precision.

In three scenarios, where the location of the rogue AP and the transmit power (low, medium and high) varied, HiGuard pinpointed the rogue to within 12 feet. Network Chemistry's RFprotect was able to detect rogues to within 10 feet in one scenario, but that accuracy stretched to 25 feet in other scenarios. Finally, the Cisco 4400 WLC/WCS identified rogues to within 20 feet in one scenario, but that accuracy wavered to 60 feet under other conditions. (See Appendix A.)

In another scenario where engineers simulated a DoS attacker in a parking lot outside a building, HiGuard tracked the attack to within 20 feet. During tesing the Cisco and the Network Chemistry systems could not demonstrate the capability to track a DoS attacker.

Another point of differentiation is around historical or forensic location tracking. The Siemens' HiGuard tracks not only active and inactive APs, it also provides tracking of historic events, such as an attack that took place on a weekend when there is no one in the building. The Cisco WLC/WCS only tracked currently active APs and offered no historical data. The Network Chemistry RFprotect was able to track active devices and also stored the last known location of APs that had been powered off, but retained no other historical or forensic data.

Management Reporting

Many IT organizations must contend with regular compliance reporting requirements imposed by government regulations such as Sarbanes-Oxley, HIPAA, or Gramm-Leach-Bliley.

Pre-defined reports and automated scanning simplify this task. Effective products deliver interactive drill-down features, as well as customizable reporting and flexible delivery frequency.

The Tolly Group examined the three WIPS products tested to determine their support for pre-formatted compliance reports and other report capabilities. (See Figure 8.)

Note: While the Cisco WCS can claim "reports" as a check box item, the content and presentation of these reports matches more closely to the dashboard information presented by Siemens' HiGuard and Network Chemistry's RFprotect. Readers should evaluate these capabilities themselves.

FIGURE 8

Standard Reports Offered and Reporting Features of WIPS Tested

Types of reports	HiPath Wireless Manager HiGuard ver. 2	Cisco 4400 WLC 4.0 and WCS 4.0 Server	Network Chemistry RFprotect 5.0
Pre-formatted compliance reports			
SOX (Sarbanes-Oxley Act)	YES	NO	NO
GLBA (Gramm-Leach-Bliley Act)	YES	NO	YES
HIPAA (Healthcare Insurance Protability and Accountability Act)	YES	NO	YES
DoD (Department of Defense)	YES	NO	YES
PCI	YES	NO	YES
Pre-formatted standard reports	YES	NO	YES
Custom reports			
Customizable sections	YES	NO	NO
Customizable database queries	YES	NO	NO
Customized reports by administrator user	YES	NO	NO

SOURCE: The Tolly Group, September 2006

WIPS products also must offer a polished set of troubleshooting capabilities to guide users through trouble spots.

Three of the most common capabilities are remote wireless packet capture, a knowledgebase for root cause analysis and radio frequency (RF) diagnostics that provide RF heat maps to identify trends and issues for radio coverage.

The Tolly Group examined the products tested for their support of these common troubleshooting capabilities. (See Figure 9.)

FIGURE 9

Troubleshooting Features of WIPS Products Tested

Types of features	HiPath Wireless Manager HiGuard ver. 2	Cisco 4400 WLC 4.0 and WCS 4.0 Server	Network Chemistry RFprotect 5.0
Dashboard	YES	YES	YES
Charts	YES	YES	NO
Remote Wireless Packet Capture	YES	YES	YES
Knowledge Base for Root Cause Capture	YES	NO	NO
RF Diagnostics using visual RF heat maps	YES	YES	YES
Forensic data storage	31 days	7 days	30+ days
Historic event tracking	YES	NO	NO
DoS attacker location tracking	YES	NO	NO
Event/alarm descriptions	Excellent	Poor	Minimal
Check Point OPSEC integration	YES	NO	NO

SOURCE: The Tolly Group, September 2006

Summary

As indicated in the beginning of this white paper, every wireless intrusion prevention system must deliver three basic sets of functionality:

- Detection and automatic classification of wireless threats
- Prevention of multiple simultaneous wireless threats while continuing to scan for new threats
- Accurate location tracking of wireless threats on a floor map

Siemens' HiGuard was the only WIPS tested that delivered on all three counts. HiGuard clearly outperformed both the Cisco 4400 WLC/WCS and the Network Chemistry RFprotect on all the measured criteria.

The Tolly Group's hands-on evaluation of the three WIPS offerings also shows that HiGuard includes incremental capabilities that make it a more versatile approach to wireless security than other products that offer just the basics.

HiGuard's management reporting, WLAN troubleshooting and RF display/visualization capabilities provide a depth of functionality that is unmatched by the other products tested.

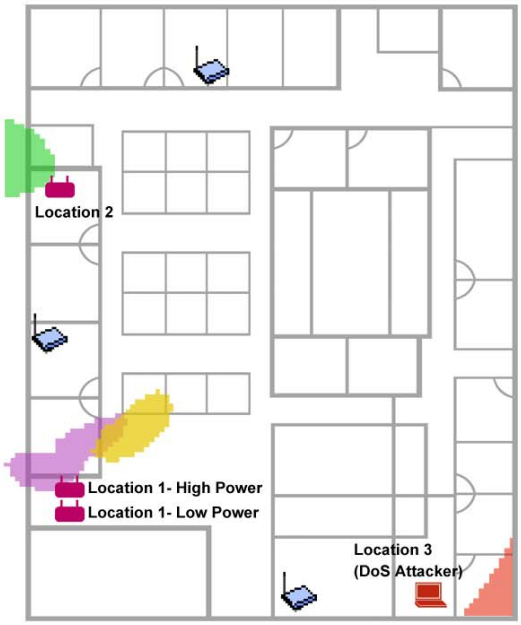
Any network operator considering the purchase of a WIPS should evaluate these advanced services, in addition to marching through the checklist of wireless security threats and how the prospective products are designed to detect and deal with those issues.

In the case of Siemens' HiGuard, prospective buyers will find a WIPS that goes well beyond the basics of identifying security threats, to offer a rich set of security capabilities and management tools to help secure wireless deployments in enterprise networks.

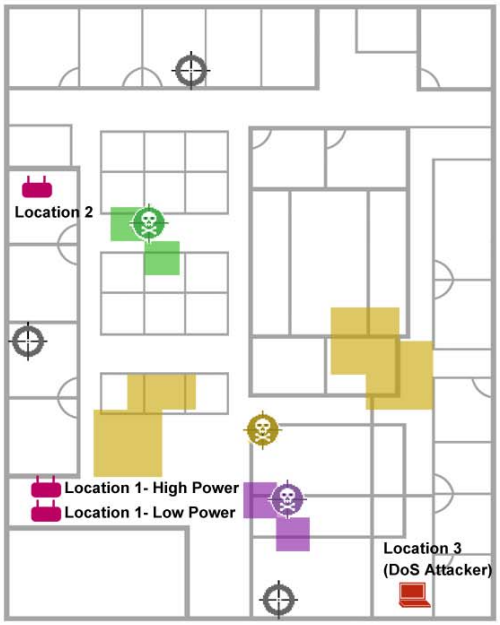
Appendix A. Location Tracking Maps

Location Tracking Predictions

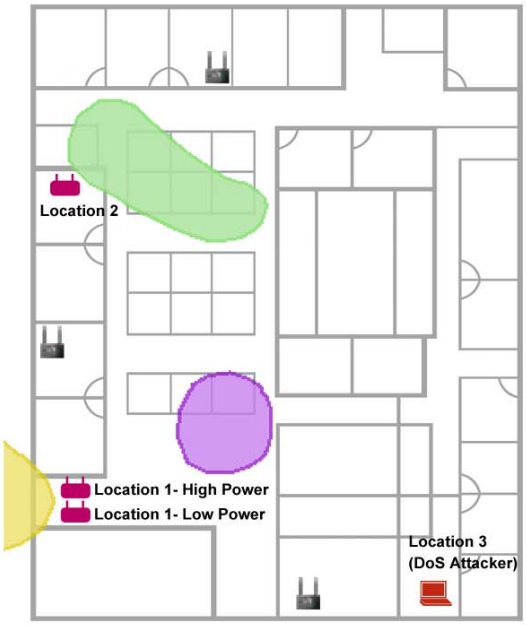
Siemens



Cisco



Network Chemistry



Sensor Locations - Legend

Siemens	
Cisco	
Network Chemistry	

Predicted Threat Locations - Legend

Location Name	AP Type	Detected Locations
Location 1	High power Cisco AP	
Location 1	Low power Cisco AP	
Location 2	Medium power Belkin AP	
Location 3 (DoS Attacker)	DoS attacker Laptop	

Appendix B. Test Tools

Wireless Access Points (APs)

Vendors: Belkin, Airlink, D-Link, NETGEAR, Cisco, Linksys
Product Name: Varies by vendor
Description: Commodity APs, chosen at random
Software/Firmware Rev Level: Varies
Test Tool Platform: N/A
Test Tool Vendor Web: By vendor
Test Tool Product Web: By vendor

Client Laptops

Vendor: Dell
Product Name: Latitude D600, D610
Description: Commodity laptops
Software/Firmware Rev Level: Varies
Test Tool Platform: Windows XP
Test Tool Vendor Web: *http://www.dell.com*

Client Wireless Network Interface Cards

Vendors: Intel, Cisco, Linksys
Product Name: Centrino, Cisco a/b/g, Linksys a/b/g
Description: Commodity wireless NICs
Software/Firmware Rev Level: Varies
Test Tool Platform: Windows XP
Test Tool Vendor Web: By vendor
Test Tool Product Web: By vendor

Network Security Tool

Vendor: US Sysadmin
Product Name: Operator
Description: A KNOPPIX bootable CD with a selection of open source network security tools
Software/Firmware Rev Level: Ver. 3.3
Test Tool Platform: Linux Kernel 2.4.31
Test Tool Vendor Web: *http://www.ussysadmin.com/*
Test Tool Product Web: *http://www.ussysadmin.com/operator/*

Information technology is an area of rapid growth and constant change. The Tolly Group conducts engineering-caliber testing in an effort to provide the internetworking industry with valuable information on current products and technology. While great care is taken to assure utmost accuracy, mistakes can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental, and consequential damages which may result from the use of information contained in this document. All trademarks are the property of their respective owners.

THE TOLLY GROUP

The authoritative, unbiased source for IT certification, research and testing

3701 FAU Blvd, Suite 100, Boca Raton, FL 33431
info@tolly.com ● phone (561) 391-5610 ● fax (561) 391-5810