



## **NETWORK ACCESS TECHNOLOGY OVERVIEW**

**FORTINET**<sup>TM</sup>  
REAL TIME NETWORK PROTECTION

[www.fortinet.com](http://www.fortinet.com)

## Contents:

THE PROBLEM	PAGE 3
CISCO NAC BACKGROUND INFORMATION	PAGE 3
TCG'S TNC BACKGROUND INFORMATION	PAGE 4
MICROSOFT'S NAP BACKGROUND INFORMATION	PAGE 6
TECHNOLOGY BACKGROUND	PAGE 8
WHAT OTHERS ARE SAYING	PAGE 9
ACCESS CONTROL TECHNOLOGY CONSIDERATIONS	PAGE 9
FORTINET'S NETWORK BASED SECURITY TECHNOLOGY	PAGE 11
FORTINET'S VIEWPOINT AND POSITION	PAGE 11
ABOUT FORTINET	PAGE 13

>> *The technology is not designed to stop malicious users or spot hacking attempts, network attacks or any other forms of malicious traffic*

## THE PROBLEM

As the newer generations of security threats endanger critical information and data systems, IT professionals are looking for advanced security solutions to help secure their network and endpoint infrastructure. With the number of vulnerabilities rising each day, the task of patching and updating every host in the enterprise has become an ongoing task that is robbing IT departments of their valuable resources. To help solve this problem, Cisco, Microsoft, and the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) subgroup recently announced the development of new technology to control network access based on the condition of the endpoint host. Many IT and security professionals believe that Cisco's Network Access Control (NAC), Microsoft's Network Access Protection (NAP), and the TCG's Trusted Network Connect technology are a step in the right direction and could help standardize the endpoint's application revision and patch levels.

As good as enforceable patch management sounds, NAC, NAP, and TNC technology is not without faults. The technology is not designed to stop malicious users or spot hacking attempts, network attacks or any other forms of malicious traffic - so it is not a replacement for existing security technologies such as Antivirus, Firewall, Intrusion Detection and Prevention, Web Content Filtering, and Anti-Spam. As of October 2004, there are three proposals (Cisco's NAC, Microsoft's NAP, and TCG's TNC) to choose from and they are not cross functional to make it easier for customers to implement. Cisco and Microsoft have agreed to work closely together to make sure their technologies are compatible, but solutions from Microsoft are not expected until late 2006 or 2007.

This document will help customers understand the offerings being proposed and discuss some of the issues that IT professionals face when trying to automate patch management. It will also show how this new technology may be complimentary to Fortinet's multi-function security platforms and how layering technologies such as NAC, NAP, or TNC may help reduce the chances of infections and attacks.

## CISCO NAC BACKGROUND INFORMATION

Cisco and many other networking and security companies have started working on a new "Network Access" technology for endpoints that is creating a lot of news in the security space. Cisco's proprietary solution is called Cisco Network Admission Control (NAC) and competes with Microsoft's Network Access Protection (NAP) technology and the Trusted Computing Group's (TCG) technology called Trusted Network Connect (TNC). These technologies attempt to accomplish the same end solution - prevent endpoints that are not up to security specifications from gaining network access. NAC is supposed to make every piece of Cisco gear a security enforcement point, where client machines must meet security and policy criteria to access a router or switch port.

Cisco's Phase I implementation was announced back in November 2003 and is

generally applicable to only Cisco router and switches for now. Cisco released some hints in June 2004 about its road map for NAC that may include offering NAC to standards bodies and other vendors by the end of the year - in effect, driving NAC as a new networking standard for a Phase II strategy. For now, Cisco has worked with several security providers such as Trend Micro, Symantec, and Network Associates to create a client-side anti-virus agent to work with their NAC enforcement technology. Cisco is making the Trust Agent available for free to all NAC partners and is asking vendors to join this partnership.

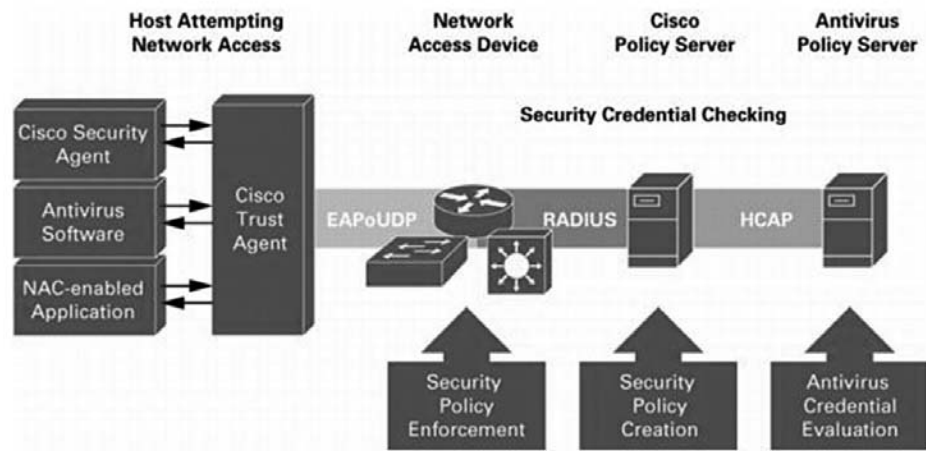


Figure 1: CTA Architecture (Courtesy of Cisco Trust Agent 1.0 Data Sheet)

Initially, Cisco NAC will only work with Windows 2000, NT and XP clients - with Linux and Solaris support by the end of 2004. If Cisco is on track with its NAC roll out, they will offer the Trust Agent API technology to the IETF some time in Q3 2004 to begin Phase II. By doing this, other vendors (aside from the three mentioned above) will have access to the technology to write drivers and inter-operate with the Cisco hardware. There has been no announcement of when and if Cisco will release the NAC technology running on its hardware to other vendors to create a unified approach for the network infrastructure piece. Only the Trust Agent has been announced as an IETF Draft candidate.

Cisco announced that its Catalyst switch line and VPN 3000 series products will be NAC-capable by the first quarter of 2005. For more information on Cisco's NAC initiative, please reference the following Cisco web page:

<http://www.cisco.com/en/US/products/ps5923/index.html>

## TCG'S TNC BACKGROUND INFORMATION

The Trusted Computing Group (TCG) formed its subgroup, Trusted Network Connect (TNC) around February 2004 and released its public information at the N+I show in Las Vegas on May 11, 2004.

The TNC strategy is very similar to Cisco's with a few differentiation points:

1. It is an open proposed draft that includes many vendors from both the security and the networking industries. This allows TNC to develop a multi-vendor solution much quicker than Cisco's approach. Even with Cisco's Trust Agent going into IETF draft in Q3, this only opens the agent to other vendors. The network enforcement is still done on Cisco switches and routers. TNC's approach is to standardize the process over all components for a multi-vendor compatible solution.

Key vendors since the development phase of TNC include:

Alcatel	Avaya	Aventail
Dell	Extreme Networks	Enterasys Networks
Foundry Networks	Funk Software	HP
ICSA	Intel	iPass
Meetinghouse	Microsoft	Netscreen
Network Associates	Nortel Networks	Sygate Technologies
Symantec	Trend Micro	Zone Labs/Checkpoint

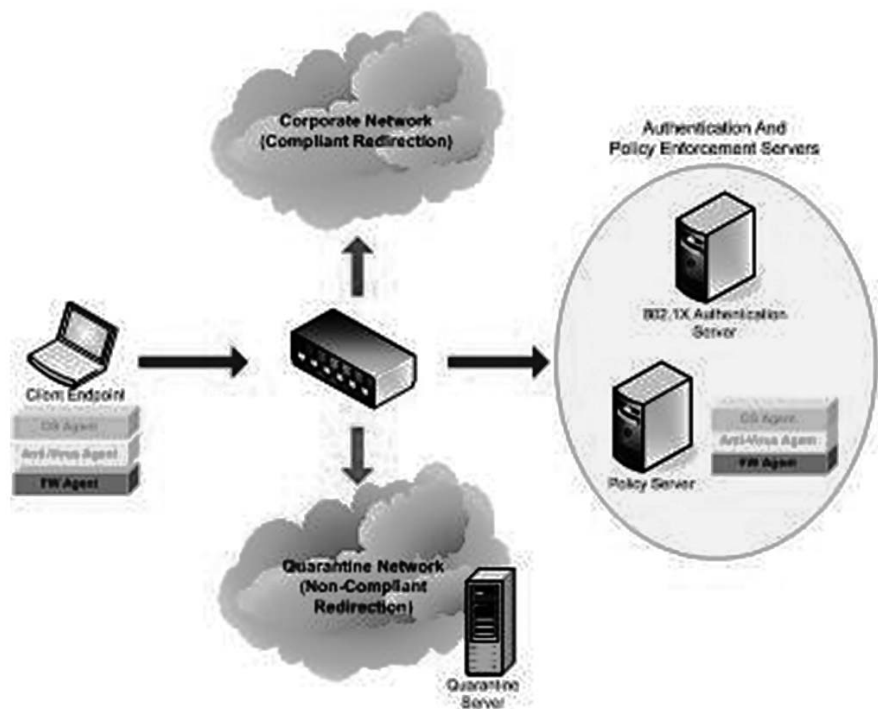


Figure 2: TCG's TNC Overview

2. TNC plans on using many of the existing standards for creating an open solution that is familiar to many customers. This includes technologies such as IEEE 802.1X Port Based Network Access Control [IEEE8021X], RADIUS, and Extensible Authentication Protocol (EAP) [RFC3748]. For applications that can not use these authentication technologies, other approaches such as web browser hijack and EAP over Point-to-Point Protocol (PPP) [RFC1661, STD051] or EAP over VPN may be considered. Unlike Cisco's approach, a proprietary Trust Agent is not required - but Cisco plans to be standards-based in the future and use a similar 802.1X approach like the TNC technology.

3. TNC's approach will depend on the OS manufacturer for the trust agent functions. TNC will rely heavily on vendors such as Microsoft to provide the common agent architecture for supporting the 3rd party vendor's agent technology. This will go a long way towards acceptance of TNC's position and early adoption by customers standardizing on Microsoft operating systems. With Microsoft's involvement in TCG and the open architecture proposed in the TNC approach, acceptance of "access control" technology may be faster with the TNC approach.

In mid October 2004, Cisco and Microsoft announced a working relationship that will help make both company's access control technology compatible over time. Microsoft's plan for its NAP technology will be through its next generation server operating system which is not due out until 2006 or 2007 - code named Longhorn. In the meantime, there will be different network access systems from various vendors supporting different enforcement techniques from either Cisco or one of the TNC vendors.

#### MORE INFORMATION ON TCG'S TNC APPROACH:

<http://www.processor.com/editorial/article.asp?article=articles%2Fp2626%2F08bp26%2F08bp26.asp&guid=&searchtype=&WordList=&bJumpTo=True>

[https://www.trustedcomputinggroup.org/downloads/TNC\\_FAQ\\_final\\_may\\_11\\_2004.pdf](https://www.trustedcomputinggroup.org/downloads/TNC_FAQ_final_may_11_2004.pdf)

[https://www.trustedcomputinggroup.org/downloads/TNC\\_NI\\_collateral\\_10\\_may\\_final.pdf](https://www.trustedcomputinggroup.org/downloads/TNC_NI_collateral_10_may_final.pdf)

### MICROSOFT'S NAP BACKGROUND INFORMATION

Microsoft's NAP technology is an extensible platform consisting of server components, client components, APIs, and quarantine resources. NAP will eventually be embedded into Windows Server to help IT professionals enforce compliance with policies for network access. Similar to Cisco and TNC's approach, Microsoft's NAP will provide a way to detect the health of an endpoint computer and either allow access to the network or redirect the client to a "restricted zone" where they can obtain the updates to become compliant. Microsoft's solution will provide the following key functions:

**Network Policy Validation** will check the state of the endpoint when they try to connect to the network. Administrators will be given the opportunity to select what to do when an endpoint is not compliant - log the violation and let the user on or quarantine the client to secure area.

**Network Policy Compliance** will allow the administrators to automatically update the noncompliant endpoints with the required OS patches or service packs using tools such as Microsoft's Systems Management Server (SMS).

**Network Isolation** will help protect network resources by restricting network access to a quarantine network or to a single resource, such as a web server

where users can download the necessary patches. The client can also be denied access if the administrator so chooses.

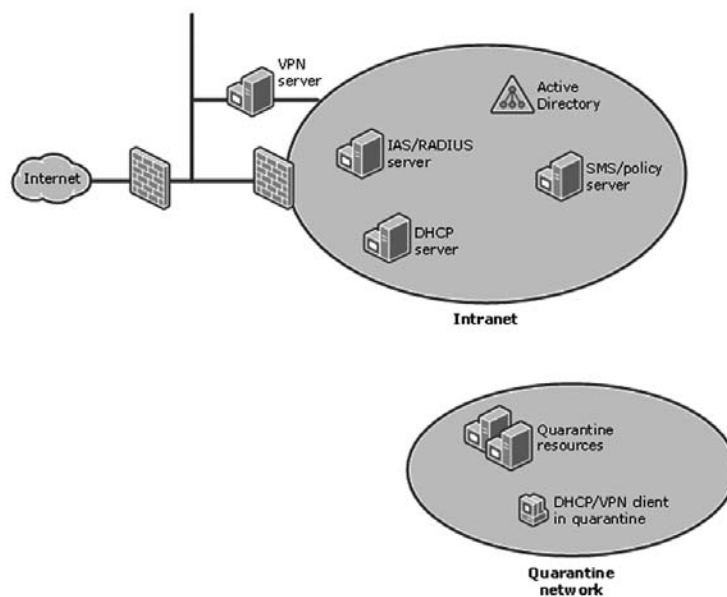


Figure 3: Microsoft NAP Overview

(Courtesy of Microsoft's Introduction to NAP for Windows Server 2003)

#### Server Components for NAP:

Quarantine Server  
 System Health Validator  
 Policy Server  
 Quarantine Policy  
 Systems Management Server (SMS)  
 Accounts Database

#### Client Components for NAP:

Quarantine Agent  
 Policy Client  
 System Health Agent

#### IMPORTANT DIFFERENCES IN THE MICROSOFT NAP PROPOSAL INCLUDE:

- NAP is designed to work with potentially any Windows application that can integrate Microsoft's APIs.
- It will only work with endpoints running Microsoft operating systems.
- It will only support Microsoft's IAS RADIUS server technology.

#### MORE INFORMATION ON THE MICROSOFT NAP TECHNOLOGY:

<http://www.microsoft.com/windowsserver2003/techinfo/overview/napoverview.mspx>

[http://news.com.com/Cisco%2C+Microsoft+in+security+showdown/2100-7355\\_3-5370427.html](http://news.com.com/Cisco%2C+Microsoft+in+security+showdown/2100-7355_3-5370427.html)

[http://news.com.com/Microsoft+spearheads+latest+security+partnership/2100-1009\\_3-5268323.html?tag=nl](http://news.com.com/Microsoft+spearheads+latest+security+partnership/2100-1009_3-5268323.html?tag=nl)

## TECHNOLOGY BACKGROUND

TCG's technology is similar to the authentication technology that many of us are familiar with today - except that it's applied to a host rather than a user. Based on a similar challenge response system, IT and security managers set policies to govern the endpoint's access to the network. Each time a host is connected to the network, they are challenged or pre-screened for compliance against the policy before gaining access to the network. Hosts can also be polled for compliance at regular intervals.

Policies can be setup to gauge access based on many factors. Examples of screening for compliance may include the endpoint's operating system and the level of system patches, if the corporate approved anti-virus program and latest virus signatures are loaded, if the local firewall policies comply with corporate standards, and so forth. Depending on the state and compliance level of the endpoint, the host may be granted full access, limited access, quarantined, or denied access. With a well written Security Policy, IT managers can now begin to police access and formalize some level of standard compliance with regards to the operating system revision, application revisions, and their patch levels.

### TNC WHITE PAPER EXPLAINING ACCESS CONTROL TECHNOLOGY:

[http://www.interop.com/lasvegas2004/pdf/lan\\_trusted\\_network\\_connect.pdf](http://www.interop.com/lasvegas2004/pdf/lan_trusted_network_connect.pdf)

Cisco's NAC technology is very similar to the proposed TNC solution, but requires Cisco proprietary components - such as their Trust Agents (available for free from Cisco), Catalyst routers and switches, and Cisco Access Control Server. The advantage of the Cisco approach is that the solution is entirely from the same vendor, so there are likely to be less compatibility issues when the technology is initially released. By not initially developing the solution with Microsoft directly, Cisco is proposing the solution to other platforms, such as Linux and Solaris by the end of 2004.

In October 2004, Cisco and Microsoft announced a working relationship to work towards a compatible solution between the two vendors. The combined solution is not expected until late 2006 or early 2007 with Microsoft's Longhorn Server platform.

### MORE INFORMATION ON THE JOINT ANNOUNCEMENT CAN BE FOUND HERE:

[http://newsroom.cisco.com/dlls/partners/news/2004/pr\\_prod\\_10-18.html?CMP=ILC-001](http://newsroom.cisco.com/dlls/partners/news/2004/pr_prod_10-18.html?CMP=ILC-001)

Microsoft's NAP solution will work only with Microsoft clients and Microsoft server technology. To fully block physical access, NAP may need to work with the various switch vendors to lock out or redirect the physical ports supporting noncompliant endpoints. Although Microsoft doesn't sell networking equipment, its dominance in the desktop and server markets gives it a strong advantage with customers standardized on its products.

As exciting as the proposed technology is, access control is still not a security module to protect the endpoint against attacks - like an antivirus application, personal firewall, or intrusion detection/prevention system. NAC, NAP, and TNC are mechanisms to authenticate an endpoint, enforce a patch revision policy, and take action against endpoints that do not qualify before giving access to the corporate LAN. NAC technology is not a real-time security protection mechanism that replaces the need for antivirus, firewall, IDS, IPS, web content filtering, spam protection, etc. and it is not completely transparent to the end user. End users must still be educated on how to obtain the latest patches once their hosts have been quarantined.

## WHAT OTHERS ARE SAYING

Many technology analysts are agreeing that the principle of "edge-based policy enforcement" is sound and that the technology is long overdue. The ability to police network access based on the endpoint's configuration and patch revision status is very attractive to many IT and Security professionals. This technology will enhance patch management and allow companies to standardize on specific OS and application configurations - which may go a long way towards stopping hosts from being infected with viruses and worms that are based on well-known vulnerabilities.

### QUOTES FROM INDUSTRY ANALYSTS AND EARLY ADOPTERS REGARDING CISCO'S NAC ANNOUNCEMENT:

- "NAC requires companies to think differently about how their networks are deployed," Kerravala said. "Most networking is reactive. Companies look backward, and ask 'What features do we have and how do we deploy them?' With NAC, they have to think in advance about what their network architecture is going to be."

"Some enterprises are suffering badly right now from infections of mobile laptops," says Mark Bouchard, an analyst with Meta Group. He says individual and joint product offerings from vendors such as Network Associates, Check Point, Nortel and Sygate already deliver what Cisco is making available next week. Also, the road map for including LAN switch support in NAC, "is not a lot different than what Enterasys talks about right now," says Zeus Kerravala, an analyst with The Yankee Group.

"What Cisco has going for it is the lion's share of the enterprise switch market," Kerravala says.

- "[NAC] could be another level of defense, but it can't be the only defense," says Ed Gotthelf, director of network architecture for UPS in Atlanta. Gotthelf says NAC "is a step in the right direction," but he says he would like to see a more industry-wide approach to LAN/WAN security.

## ACCESS CONTROL TECHNOLOGY CONSIDERATIONS

As good as endpoint access control technology is and welcomed, there are still some considerations before full enterprise-wide adoption can happen. Some considerations for IT and security professionals include (but not limited to):

- Not all network switches and routers may support NAC, NAP, or TNC technology. Upgrading network switching or routing equipment to fully support 802.1X and EAP may be very costly for many companies.
- Will there be solutions for both wired and wireless infrastructure as well as local and remote access enforcement?
- Not all hosts will support the necessary agents to work with the policy servers. Will there be agents readily available to support the most popular operating systems in a reasonable time frame?
- Many IT departments will wait and fully test OS patches and application upgrades before rolling them out to prevent disruption or breaking of existing corporate applications. This delay may make them vulnerable if their access policies do not enforce the latest security patches.
- IT departments that rush to deploy the latest patches or upgrades to secure their companies may risk breaking critical or legacy applications - causing "self induced" downtime.
- Users will have to be educated on how to obtain the latest patches and learn how to perform the upgrades when their hosts are quarantined. Although automated software installation programs such as Microsoft's SMS may be used, many companies and users may still rely on IT resources to help keep their systems patched. Users may be intimidated by performing OS and application patching.
- How will this work in public networks such as libraries, educational networks, Hot Spot environments where there is no IT support?
- Having the latest anti-virus signatures and OS patches will not guarantee immunity to the latest zero-hour attacks, worms, trojans, viruses, and sophisticated blended attacks. Installing host based firewalls, IDS or IPS in addition to popular anti-virus applications on each endpoint will greatly help, but is still too cost prohibitive for many enterprises to deploy and manage.
- Access control technology will not prevent users with the latest patches from probing, hacking, or attacking network resources. It will not spot probing, denial of service, intentional hacking, etc. from disgruntled employees, visitors, or any other users who gain access to the network. A good example of this fact is public access networks and educational networks where hackers can gain access to the network, by meeting the patch level policy, then launch attacks or probes against other systems and users.

*>> Having each endpoint patched properly enhances a defense-in-depth security strategy and is critical to a solid defense against modern threats.*

## **FORTINET'S NETWORK BASED SECURITY TECHNOLOGY**

Fortinet's technology provides a comprehensive multi-tiered solution that is fully complimentary to Cisco's Network Access Control, Microsoft's Network Access Protection, and TCG's Trusted Network Connect technology. Each company's requirements will vary and their policies regarding patch management will affect the success rate of endpoint security technology. Waiting too long to enforce a vulnerability will leave the company's assets exposed. Creating policies that enforce them before thorough testing runs the risk of breaking stable applications.

In August 2004, many companies rushed to upgrade to Microsoft XP's Service Pack 2 (SP2). The long awaited service pack was full of new security features that were meant to help secure corporate resources. The rush to implement the service pack without thorough testing ended up breaking many stable applications that were required to perform critical business. As reported by many Internet sources, hundreds of applications were "broken" and made incompatible after the installation of SP2 - causing many hours of repair work for IT and desktop professionals. Companies who read about the incompatibility held off upgrading and scheduled thorough testing of all corporate applications before installing the service pack - leaving them vulnerable to threats that SP2 was supposed to help solve.

Having each endpoint patched properly enhances a defense-in-depth security strategy and is critical to a solid defense against modern threats. NAC, NAP, and TNC will allow the customer more options when designing a secure networking environment. Combined with Fortinet's Network-Based security technology, customers can implement the latest protection in real-time to safeguard their corporations against the world's most recently discovered threats without having to worry about disrupting their existing host environments.

Fortinet's global real-time updating service (FortiProtect) automatically updates every FortiGate network security device with the latest Antivirus and Attack Signatures to give customers additional time to thoroughly test their OS and application patches before enforcing them with NAC, NAP, or TNC policies. This approach greatly lowers the chances of implementing patches or service packs that can severely disrupt their computing environment causing outages and impacting user productivity. Simply stated, Fortinet's security solutions allow customers to increase their levels of corporate security without adversely adding more risk and potential downtime.

## **FORTINET'S VIEWPOINT AND POSITION**

Fortinet sees NAC, NAP, and TNC technology as fully complimentary to its FortiGate and FortiClient technologies and views the work being done by TNC, Microsoft, and Cisco as a deeper push towards a true "defense-in-depth" security model - where different types of security mechanisms are layered to provide an overall hardening of the network infrastructure. Fortinet's reasoning is quite

*>> Fortinet views this technology as a strong step in the right direction towards a more compliant and standardized network.*

simple. Network access technology is used to determine an endpoint's state before granting network access. It is not technology to help protect the endpoint from being attacked and the customer must still deploy FW's, IDS/IPS, AV, etc. to every client to take advantage of the automated enforcement capabilities offered in network access technologies.

Fortinet views this technology as a strong step in the right direction towards a more compliant and standardized network. Cisco NAC and the work from Microsoft and the TCG is not a replacement for network-based real-time content security solutions provided by Fortinet. These technologies help to compliment the protection offered by the FortiGate products: stateful firewall, VPN, IDS & IPS, antivirus, web content filtering, spam filtering and traffic shaping. Fortinet believes that in order to identify, contain, and stop blended and fast spreading threats in all areas of the corporate network, a combination of security approaches must be adopted at all layers of the corporate network - endpoints, strategic choke points, and perimeter points.

For the reasons mentioned in the "Access Control Technology Considerations" section, not all companies will be able to take advantage of quick immediate updates - as suggested by the NAC, NAP, and TNC concept. Having the ability to perform full content inspection against the latest threats and attacks without the risks of implementing untested patches will be very critical to companies that are operating mission critical applications. These customers can not afford downtime for any reason and Fortinet's security philosophy was designed around this premise from the very beginning.

Fortinet's latest product offering provides customers with the "Dynamic Threat Prevention System" that combines the Intrusion Detection and Prevention functions to create a stronger defense against known and unknown attacks. The Dynamic Threat Prevention technology can be applied on a per-firewall policy basis to apply the security technology where the customer needs it most - detecting and optionally blocking malicious applications and content. Fortinet's FortiProtect and FortiGuard services automatically provide customers with the latest detection signatures in real time to create an unparalleled security platform that is up-to-date against the latest threats. Performing real-time updates at the network level dramatically lowers the maintenance overhead that is normally associated with trying to keep up-to-date all the endpoint security applications. It also greatly improves the capabilities of stopping the latest security threats and vulnerabilities at the network perimeter before they have a chance to enter the corporate network.

At this time, Fortinet will continue to proactively monitor and investigate the work being done by Cisco, Microsoft, and the TNC. As the concept of enforceable automated patch management matures and standards evolve around these practices, Fortinet will research, evaluate and develop the necessary strategy to incorporate access control technology.

## ABOUT FORTINET (WWW.FORTINET.COM)

Fortinet is the confirmed leader of the Unified Threat Management market. The company's award-winning FortiGate™ series of ASIC-accelerated antivirus firewalls, winner of the 2004 Security Product of the Year Award from Network Computing and the 2003 Networking Industry Awards Firewall Product of the Year, are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from e-mail and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time - without degrading network performance. FortiGate systems are the only security products that are quadruple-certified by the ICSA (antivirus, firewall, IPSec, NIDS), and deliver a full range of network-level and application-level services in integrated, easily managed platforms. Named to the Red Herring Top 100 Private Companies, Fortinet is privately held and based in Sunnyvale, California.

### SALES

Please contact us at [sales@fortinet.com](mailto:sales@fortinet.com)  
or phone toll-free in the U.S. (866) 868-3678 or +1(408) 235-7700.

### POTENTIAL PARTNERS

Please contact us at [partners@fortinet.com](mailto:partners@fortinet.com) or visit us at [www.fortinet.com](http://www.fortinet.com).

Copyright 2004 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiClient, FortiGuard, FortiOS, FortiProtect, and FortiASIC are registered trademarks of Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. WPR1130410

