

# DNAC TECHNICAL OVERVIEW

## InfoExpress Network Access Control



**infoexpress**

T. 650.623.0260 F. 650.623.0268 [www.infoexpress.com](http://www.infoexpress.com)

© 2008 InfoExpress, Inc.

The information contained herein is the property of InfoExpress, Inc. and may not be copied, used or disclosed on whole or in part, stored in a retrieval system or transmitted in any form or by any means (electronic, mechanical, reprographic, recording or otherwise) without the prior written permission of InfoExpress, Inc.

CyberArmor, CyberGatekeeper Remote and CyberGatekeeper LAN are registered trademarks of InfoExpress Inc. All other product names are registered trademarks of their respective owners.

Document ID: WP08-0124-01

DNAC's approach to enforcement is based on a "neighbourhood watch" system. Endpoints that have passed audit and are compliant with the security policy are considered trusted, and can become enforcers. The enforcers use a combination of active and passive detection mechanisms to discover a new endpoint when it joins the network. When a new DHCP based endpoint connects to the network for example, it will send out a DHCP DISCOVER request. This broadcast packet will be seen by all enforcers on the endpoint's subnet. Statically addressed endpoints will send out ARP requests, which are also broadcasts, to locate endpoint's and routers with whom they wish to communicate. Enforcers also periodically scan the network to detect new systems as they connect.

When an enforcer sees a new endpoint join the network, it checks to see if an endpoint has passed audit or is whitelisted. If neither of these are true the endpoint is considered rogue, and the enforcers take action to quarantine the endpoint. Any endpoint – with an Agent or not – is prevented from obtaining full network access until it has passed audit, unless it has been whitelisted.

DNAC uses a "defense in depth" approach to network access control, combining both client side drivers and ARP redirection to form a complete solution. ARP is a basic, well understood IP standard and DNAC uses it such that it does not interfere with other (non-enforced or passing) endpoints in any way.

DNAC will fully enforce all endpoints with no additional configuration or network changes, including Windows 95 through Vista, Linux, Mac, network devices and hardware appliances. This is possible because DNAC uses ARP in a way that will not trigger security alarms from personal firewalls and host IDS/IPS.

Once a rogue endpoint is detected, an enforcer will automatically (and regularly) update the ARP table of the rogue and anything it attempts to communicate with. All traffic to and from the rogue is now configured to pass through the enforcer. This will have the immediate effect of restricting its network access to the ACL you have configured, as the enforcer will only forward packets which are permitted by the ACL.

The enforcers use directed ARP - not ARP broadcasts - to enforce endpoints. This means that the traffic load is greatly reduced, and only rogue endpoints are redirected via ARP. Valid systems that are permitted to use the network will not see any sort of unusual network traffic. Rogue endpoints - the ones you want to keep off your network as they may be causing you harm - are the only systems that DNAC quarantines via ARP redirects.

Static ARP entries will not help a rogue gain unauthorized access. The enforcer will still observe the attempted communication and the ARP updates it sends will override any static entries on the rogue, as per the standard.

The enforcer also has the ability to send TCP resets to the rogue (and the rogue's destination), to shut down any prohibited communications.

These methods, paired with the IM driver installed on trusted endpoints, provide a layered approach to restricting traffic to and from rogue endpoints.

This approach is augmented by the DNAC IM driver, which is installed on all endpoints by default. Endpoints with this driver do not need to have their packets redirected, as the driver automatically prevents these passing endpoints from communicating with any rogue, thereby reducing the dependence on ARP.

Administrators can quickly and easily identify which resources an endpoint has access to, when it is quarantined. This may range from full Internet access to limited corporate network access, permitting only selected services such as anti-virus updates or patch downloads to be available to the endpoint.

## A Simple Example

We have two hosts, Host A and Host B on a class C network. Initially, let's assume DNAC is not installed, to set a baseline. When Host A wants to communicate with Host B it'll send out a broadcast ARP to try to find the destination MAC address for Host B's IP address. Host B will see the broadcast, and reply to it, telling Host A how to get in touch. From there, communications can proceed between the two hosts.

Now let's introduce DNAC. The first steps are still the same, Host A ARPs for Host B, and Host B replies. However the enforcer – who saw Host A's ARP and knows it is a rogue – also replies to the ARP request, telling Host A that it is in fact Host B. That is, the enforcer replies to the ARP request giving its own MAC address as the match for Host B's IP address. The enforcer sends that reply several times to ensure that Host B's ARP update is immediately overwritten, and will periodically re-send this reply to ensure that the redirection stays in place. This will cause Host A (the rogue) to communicate with the enforcer any time it wants to communicate with Host B, thereby preventing it from gaining network access.

In addition to replying to Host A, the enforcer will also send an ARP update to Host B, preventing it from communicating with Host A in the same manner described above. At this point, the enforcer “owns” both sides of the conversation, and can apply the access control list that has been defined by the administrator, allowing only limited access to selected resources.

There's also a slight variation to this scenario, and that is when Host B is on a different subnet than Host A. Again, Host A will ARP for Host B's MAC address, but since ARP is a layer two protocol, it will not extend beyond the current subnet, and will never reach Host B. However, the local router will recognize that this is an “off subnet” ARP request and it will automatically respond with its own MAC address. In effect, this tells Host A to send all off subnet traffic to the router, which can then forward it on to its final destination (Host B in this case).

If we now inject DNAC into the mix, the process stays the same, except the enforcer now redirects Host A and the router, instead of Host A and Host B. The ARP packets sent out by the enforcer are not broadcasts, and are updates only for the single host entry, so only quarantined endpoints will be affected by the ARP changes made on the router.

## For More Information

InfoExpress is the leader in network access control. For more information on how the CyberGatekeeper Suite can increase security while lowering the cost to protect your network, please visit [www.infoexpress.com](http://www.infoexpress.com) or contact us at 613.727.2090 or at [sales@infoexpress.com](mailto:sales@infoexpress.com).