

Solution Guide

Secure Access and InfoExpress CyberGatekeeper

Denzil Wessels
Technical Marketing Engineer



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 351058-001 Aug 2004

Contents

Contents	2
Executive Summary	4
IVE Introduction	4
NetScreen Instant Virtual Extranet.....	4
NetScreen Secure Access Appliance.....	4
InfoExpress Products.....	5
InfoExpress CyberGatekeeper.....	5
NetScreen Secure Access combines with CyberGatekeeper	5
Configuration	6
NetScreen Instant Virtual Extranet.....	6
InfoExpress	7
Building a Package for upload to the SSL VPN	8

Executive Summary

Juniper Networks NetScreen Secure Access combined with InfoExpress's CyberGatekeeper allows the administrator to define policies that the connecting endpoint needs to comply to before allowing access. The integration leverages the Juniper Networks Server Integration Interface to deploy and execute security software on the endpoint.

IVE Introduction

NetScreen Instant Virtual Extranet

The IVE Platform is the foundation of the NetScreen Secure Access (NS-SA) family of SSL VPN appliances. The NetScreen Instant Virtual Extranet (IVE) platform is the software foundation of NetScreen's hardened Application Security Gateways and enables NS-SA appliances to plug seamlessly into an enterprises' existing security infrastructure.

NetScreen Secure Access Appliance

The NetScreen Secure Access (NS-SA) Appliances provide a complete range of enterprise-class scalability, high availability, and security functionality for customers seeking to cost-effectively extend secure access to network resources. Customers benefit the ubiquity that SSL VPN's are known for, as well as from redundancy and scalability, with clustering capabilities that provide greater aggregate system throughput and seamless stateful failover.

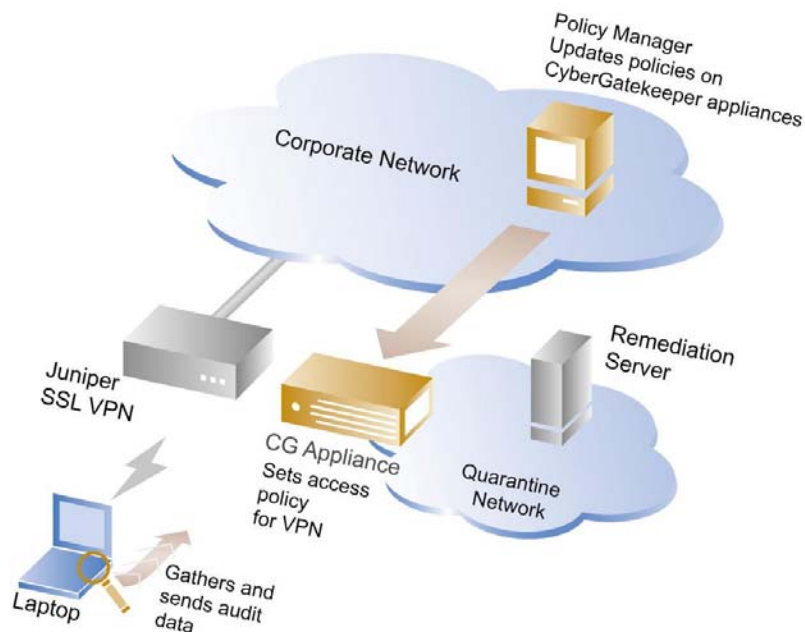
InfoExpress Products

InfoExpress CyberGatekeeper

The CyberGatekeeper solution from InfoExpress audits, quarantines, and remediates non-compliant endpoints before granting access to the corporate network. By using the network infrastructure to perform this task, the CyberGatekeeper solution is scalable and has no impact or potential to bottleneck the traffic flowing through the network. Supported network access methods include SSL and IPsec VPNs, LAN switches, WLANs, and remote access dialup.

NetScreen Secure Access combines with CyberGatekeeper

The integration between CyberGatekeeper and the Juniper Host Checker API extends the coverage to ensure that the Juniper SSL VPN will allow only those endpoints compliant with policies into the network. This integration ensures the check occurs transparently and quickly before allowing the endpoint to access the network. In the event that the endpoint falls out of compliance during a SSL VPN session, this solution will deny access to the network.



Configuration

NetScreen Instant Virtual Extranet

Once the policy has been created (under the InfoExpress configuration,) it will then get uploaded to the IVE.

- Click on Configuration...Security...Host Checker
- Click on “New 3rd Party Policy”
- Type the name, and then browse for the InfoExpress policy.
- Click save changes.

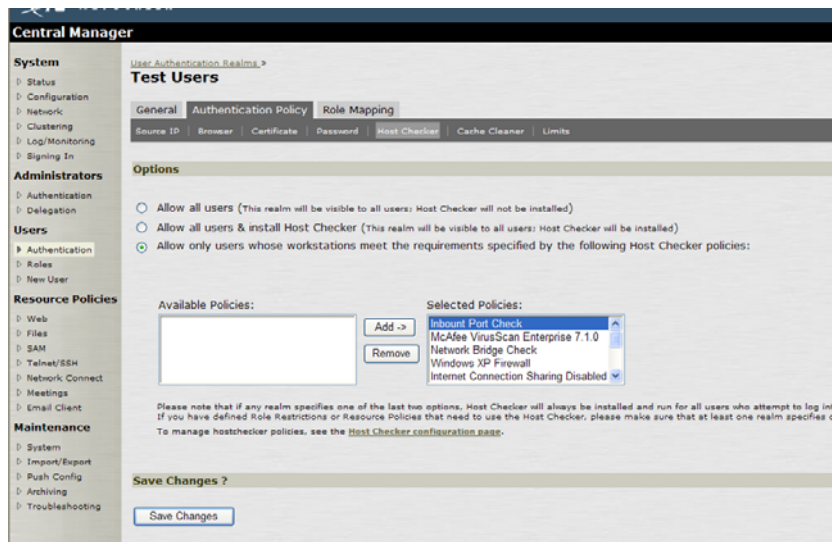


Host Checker Policies Applied to Authentication Realm

This is a screen shot of all the above Host Checker policies being applied to an authentication realm.

An administrator would go to Users...Authentication...“realm name”...Authentication Policy...Host Checker

They would then select the InfoExpress policy and click the add button. This will add it to the list of checked policies.



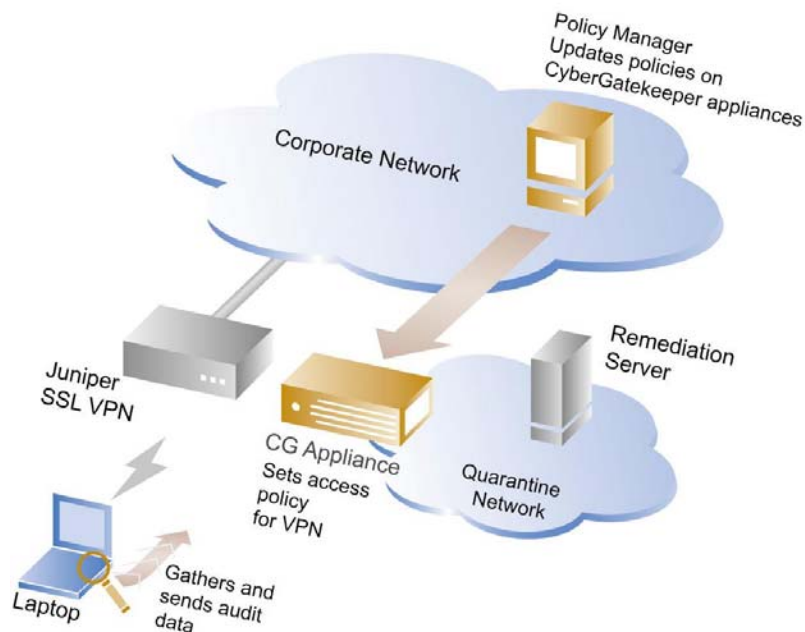
InfoExpress

Solution Components:

- CyberGatekeeper Policy Manager (CGPM, all versions)
- JHC Builder (version 1.0 or higher)
- CyberGatekeeper Server Appliance (CGS, all versions)

Install CGPM and the Juniper HC Builder package.

Install the CGS appliance. CGS must be installed in parallel with the Juniper VPN, with the outside NIC and IP address accessible to remote systems, on port 11698. This is the port and IP address that audits will take place over the Internet.



Building a Package for upload to the SSL VPN

1. From CGPM, create policies and distribute to CyberGatekeeper servers, build an agent, and verify behavior as usual.
2. To create a package to upload to the Juniper SSL VPN, run the JHC Builder. This can be found in the installation folder or from:

Start -> Programs -> CyberGatekeeper Policy Manager -> JHC Builder.

3. Enter the configuration information as per your CyberGatekeeper server configuration as appropriate, then click OK. This builds a package that can be uploaded to the Juniper SSL VPN to enforce policies which have been distributed to the CGS appliance.