

Solution Guide

Secure Access and Sygate On-Demand Agent

Denzil Wessels
Senior Marketing Engineer



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

Part Number: 351056-001 Aug 2004

Contents

Contents	2
Executive Summary	4
Perspective	4
IVE Introduction	4
NetScreen Instant Virtual Extranet.....	4
NetScreen Secure Access Appliance.....	4
Sygate Products.....	5
Sygate On-Demand Agent.....	5
NetScreen Secure Access combines with On-Demand Agent	5
Configuration	6
NetScreen Instant Virtual Extranet.....	6
Custom UI.....	6
Host Checker	6
Two Different Realms.....	6
Two Different Sign-In Policies	6
Sygate On-Demand Agent.....	7

Executive Summary

Juniper Networks NetScreen Secure Access appliances combined with Sygate On-Demand Agent enables enterprises to secure applications by ensuring the integrity of endpoints and protecting the data that is transmitted to them. This also encompasses the enforcement of data that has been delivered getting encrypted and then removed upon disconnect.

Perspective

The fundamental shift from client-server to Web-based applications has profoundly changed the way employees, business partners, customers, and suppliers access and utilize corporate information. In a client-server world, corporate information is protected by securing corporate-owned devices (using Sygate Secure Enterprise) and authenticating the user. In contrast, clientless Web-based applications and services can be accessed from any computer, including employee-owned computers, airport kiosks, hotel business center computers, and supplier systems. On these third-party-owned computers, the corporate security organization has no method to verify the security of that computer, to protect the information provided by the Web application, to erase the information at session termination, or to protect the entire session from malicious code.

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.

Sygate Products

Sygate On-Demand Agent

The Sygate On-Demand Agent enables enterprises to secure Web applications by ensuring the integrity of endpoints and protecting the data that is transmitted to them. The Sygate On-Demand Agent is downloaded from the Web application or SSL VPN box at connection time to the endpoint, eliminating the need to have pre-installed client software to secure data on third-party owned systems. The connection is only allowed if the endpoint is fully compliant with security policy and the appropriate On-Demand data protection components are in place. Sygate On-Demand works seamlessly to protect endpoints connecting to Webmail, SSL VPN, Portals, Financial /Healthcare/HR applications, and ERP systems.

NetScreen Secure Access combines with On-Demand Agent

Sygate On-Demand Manager creates a Web page containing the Sygate On-Demand Agent download. The Sygate On-Demand Agent download Web page is then installed on the Secure Access Appliance. When a user connects to the IVE platform, the Sygate On-Demand Agent (SOA) is downloaded and launched on the endpoint. Once launched, SOA verifies the integrity of the endpoint including antivirus software, personal firewall, service pack, and patch/hotfix policies. After completing the Host Integrity verification process, SOA creates a Virtual Desktop environment.

From within that virtual environment, SOA launches the login process to the IVE platform from a Web browser in the Virtual Desktop. The user is then authenticated and authorized by the IVE platform. The user can then access corporate resources such as e-mail or corporate servers as defined in the resource policies on the IVE. When the session to the Web application is complete or times out after a configurable interval, SOA can either automatically erase all data from the session or create an encrypted and password-protected virtual desktop environment that remains on the computer.

Configuration

NetScreen Instant Virtual Extranet

To use the Sygate On-Demand Agent to secure ser access to the IVE, the On-Demand Agent needs to be made accessible from the IVE sign-in pages.

You will need to configure the following:

Custom UI

You will have to add the Sygate On-Demand Agent to a Custom UI ZIP file that will get uploaded to the IVE. This file will have a link to the index.htm which will launch and run the Sygate On-Demand Agent and the virtual desktop.

In the loginpage.shtml you will need to remove the login form (username and password fields) and add a link to the On-Demand Agent. The link to add would be

```
<a href="On-DemandAgent/index.htm">Run the Sygate On-Demand Agent</a>
```

You will also have to copy the On-DemandAgent directory from the folder where the On-Demand Manager is installed to. This will need to be added to the ZIP archive that contains the custom UI.

Once this is complete this will need to be uploaded to the IVE for the "insecure" page.

Host Checker

Host Checker needs to be configured to check to see if the On-Demand Agent is running. To do this it will need to be configure to check for the two following items:

1. That the cclient.exe process is running.
2. The existence of the registry key: HKEY_CURRENT_USER\SSPisRunning = 1

Two Different Realms

There will be two distinct sign-in URL's that will have to be created.

1. On-Demand Agent deployment page which will be referred to as the "insecure" sign-in page.
2. Secure sign-in page which will be called "secure." This page will deploy Host Checker and check for the presence of the On-Demand Agent before allowing a user to submit their credentials to authenticate.

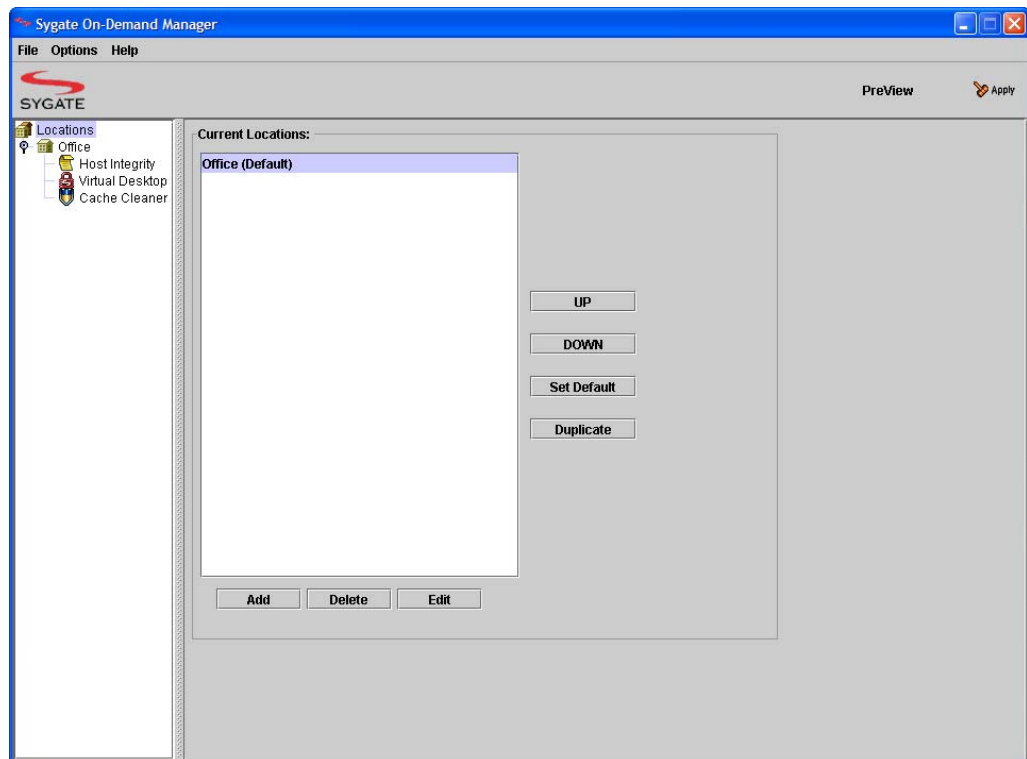
Two Different Sign-In Policies

There will be two distinct sign-in policies.

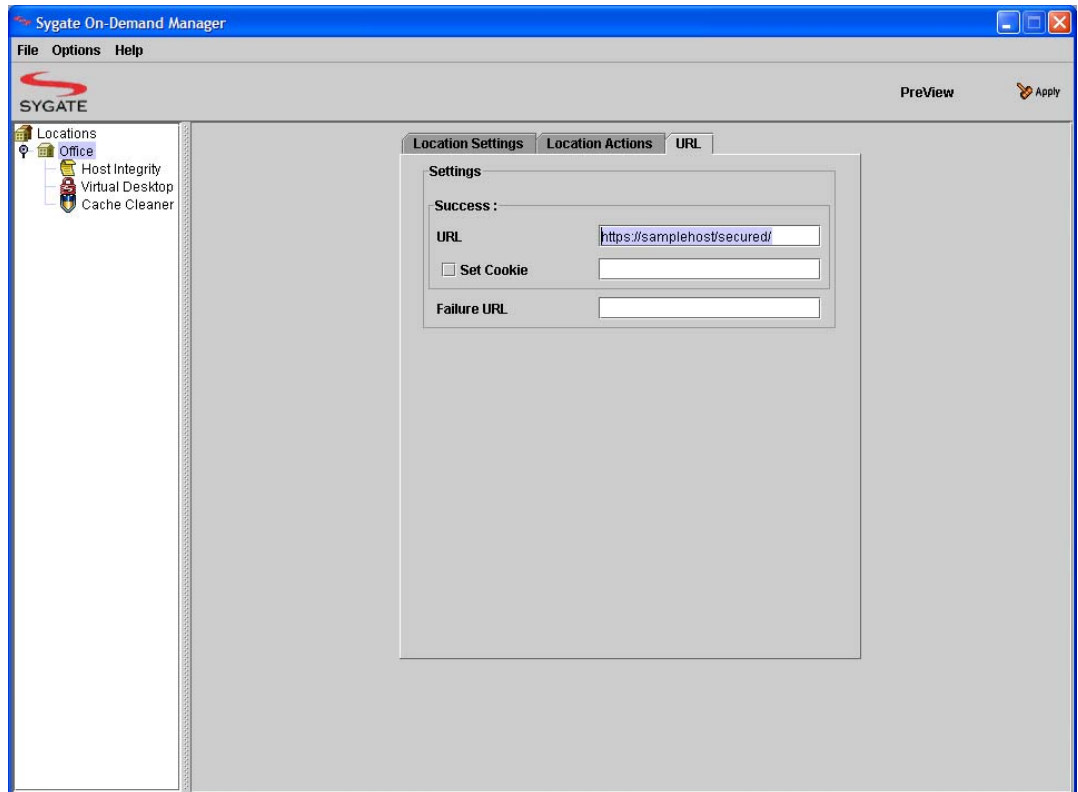
1. “Insecure” sign-in policy which will have the Custom UI that contains the Sygate On-Demand Agent. (it will refer to it as: <https://sahost/>)
2. “Secure” sign-in policy which will have the regular UI and will not need Custom UI. (It will be referred to as <https://sahost/sygateondemand>) All users connecting to this URL will need to have the Sygate Virtual Desktop running. That will be enforced by Host Checker. All users will map to the “Secure” realm.

Sygate On-Demand Agent

You will need to use the Sygate On-Demand Manager to create the “Virtual Desktop” environment and the policies that need to be adhered to for access to the IVE.



In the Office section under the URL tab, you will add the secured sign-in page of the IVE. Make sure that “Set Cookie” is not checked.



Most of the configuration is going to be done under the Host Integrity section of the On-Demand Manager. This is where you will define what policies the endpoint will have to meet for the Agent to run.

Please see the On-Demand Manager Documentation for further assistance with creating policies.

Once you have the On-Demand Manager configured, you have to copy the On-DemandAgent directory and all of its contents to your Custom UI folder.