TREND MICRO™

InterScan™ Web Security As A Service
Getting Started Guide

Total Web Protection – Everywhere and All the Time
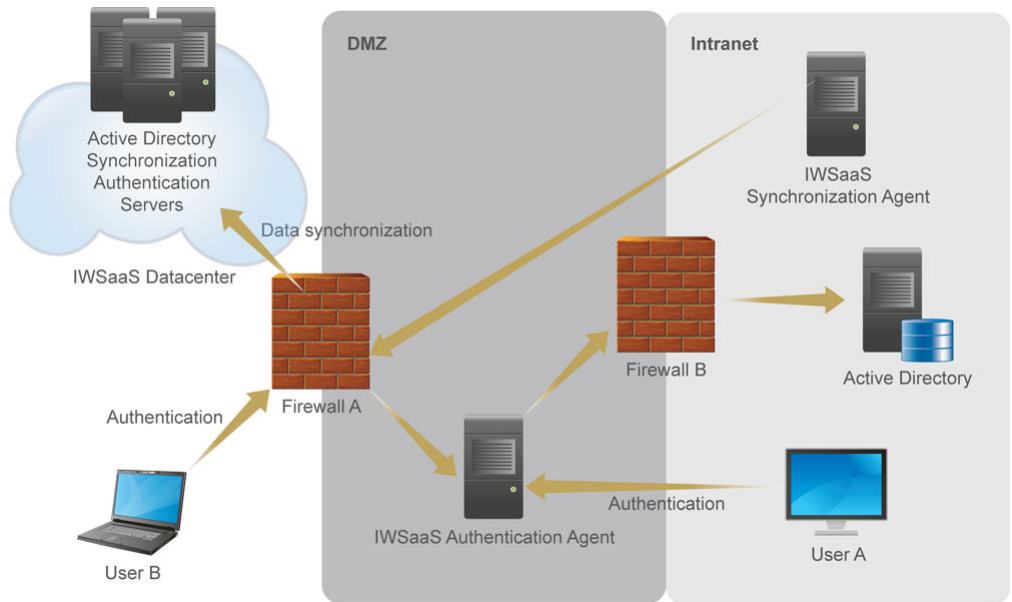
Protected Cloud   Web Security

Authenticating Users Using Agents

Use this method of user authentication if you do not have a SAML server, but still want the same level of security that SAML Authentication provides.

Specifying Ports for the Authentication Agent

Procedure

1. Install the IWSaaS Synchronization Agent in your Intranet.

    The Synchronization Agent connects to your Active Directory to sync user and group data with IWSaaS. The data transmits over the HTTPS protocol on port 443 and this outgoing port is usually open on Firewall A by default, as depicted in the graphic above.

2. Deploy the IWSaaS Authentication Agent in the DMZ.

3. On Firewall A, open incoming port 443 to allow any IP to connect to the IWSaaS Authentication Agent.

4. On Firewall B, open incoming port 389 (or 636 when SSL is enabled in the Active Directory) to allow IWSaaS Authentication Agent connect to the Active Directory.

> **Note**
>
> Putting the Authentication Agent in the DMZ allows user authentication regardless if they are inside the corporate network (User A) or outside of it (User B). But if you deploy the Authentication Agent in the Intranet, only User A--who is inside the corporate network, can authenticate and login to IWSaaS.

Source	Destination	Firewall settings
Intranet	IWSaaS services	Outbound port 443 on Firewall A (normally open)
Internet	IWSaaS Authentication Agent in DMZ	Inbound port 443 on Firewall A
IWSaaS Authentication Agent in DMZ	Active Directory Server	Inbound port 389 on Firewall B (or 636 when SSL is enabled in the Active Directory)

5. Deploy the IWSaaS Synchronization Agent to synchronize user and group data with IWSaaS.

    See *Configuring the Synchronization Agent on page 45*.

Specifying Agent Active Directory Authentication

Location: Administration > Users and Authentication > Active Directory

Procedure

1. Enable Active Directory and then click **Agent**.